dpANS

Project T10/1895-D

Revision 00d
27 August 2008

Information technology - Automation/Drive Interface Commands - 3(ADC - 3)

T10 Technical Editor:

Paul Stone
Quantum Corporation
141 Innovation Drive
Irvine, CA 92617
USA

Telephone: 949-725-1874
Fax: 949-856-7799
Email: paul.stone@quantum.com

Reference number
ISO/IEC XXXXX-XXX : 2008
ANSI INCITS.*:2008**

Printed Wednesday, August 27, 2008 1:59 PM

Points of Contact:

T10 Chair
John B. Lohmeyer
LSI Logic
4420 Arrows West Drive
Colorado Springs, CO 80907-3444
Tel: (719) 533-7560
Fax: (719) 533-7183
Email: lohmeyer@t10.org

T10 Vice-Chair
Mark S. Evans
Western Digital
5863 Rue Ferrari
San Jose, CA 95138
Tel: (408) 363-5257
Fax: (408) 363-5139
Email: mark.evans@wdc.com

INCITS Secretariat
INCITS Secretariat
1250 Eye Street, NW Suite 200
Washington, DC 20005
Telephone: 202-737-8888
Facsimile: 202-638-4922
Email: INCITS@itic.org

T10 Web Site www.t10.org

T10 Reflector To subscribe send e-mail to majordomo@T10.org with ‘subscribe’ in message body
To unsubscribe send e-mail to majordomo@T10.org with ‘unsubscribe’ in message body
Internet address for distribution via T10 reflector: T10@T10.org

Document Distribution
Global Engineering
15 Inverness Way East
Englewood, CO 80112-5704
Telephone: 303-792-2181 or
800-854-7179
Facsimile: 303-792-2192

Revision Information

1 Revision History

1.1 Revision 0 (28 February 2008)

Incorporated the following proposal approved at the January 2008 T10 teleconference. See the ADI working group meeting minutes 08-098r0:

- 08-029r2, Automation encryption control

Minor edits by Paul Entzel in Table 43 (“Fibre Channel speed values“) and 4.3.3 (“Remote SMC device server operation”). Minor edits by Paul Stone in 3.1.44 (“SMC Logical Unit”) and Table 56 (“ADC device VPD page codes”).

1.2 Revision 0a (5 March 2008)

Printed with hyperlinks enabled.

1.3 Revision 0b (23 April 2008)

Incorporated the following proposal approved at the March 2008 T10 meeting. See section 9.3 of the ADI working group meeting minutes 08-151r1:

- 08-119r0, Automation encryption control corrections

Incorporated the following editorial changes:

- Change reference to TARGET PORT field to indicate PRIMARY PORT INDEX field.
- Fix incorrect PAGE LENGTH field in Table 67, Data Encryption Parameters Complete page.
- Other minor changes.

1.4 Revision 0c (25 June 2008)

Incorporated the following proposals approved at the May 2008 T10 meeting. See sections 10.3 and 10.4 of the ADI working group meeting minutes 08-223r0:

- 08-195r2, Host Reported Error Additional Information
- 08-200r1, Clarifications for automation encryption control

Also incorporated the following editorial changes:

- Changed “Parameters Request Sequence Identifier” in Table 23 to ”Parameters Request Error Sequence Identifier” in order to match 08-029r2 (transcription error).
- Other minor changes.

1.5 Revision 0d (August 27 2008)

Incorporated the following proposal approved at the July 2008 T10 meeting. See section 08-022 of the ADI working group meeting minutes 08-291r1:

- 08-226r1, Add Port and Node Name to Fibre Channel Port Status Data

ANSI (r)
INCITS.*:2008**

American National Standards for Information Systems -

Automation/Drive Interface Commands - 3

Secretariat
InterNational Committee for Information Technology Standards

Approved mm dd yy

American National Standards Institute, Inc.

Abstract

This standard specifies the device model and functional requirements for the SCSI automation/drive interface device type. This standards permits the SCSI automation/drive interface device type to communicate with application clients and defines the commands and data exchanged in such communications.

This standard does not contain material related to the service delivery subsystem that is used to transport the commands, command parameter data, command response data, and status specified in this standard.

American National Standard

Approval of an American National Standard requires verification by ANSI that the requirements for due process, consensus, and other criteria for approval have been met by the standards developer. Consensus is established when, in the judgment of the ANSI Board of Standards Review, substantial agreement has been reached by directly and materially affected interests. Substantial agreement means much more than a simple majority, but not necessarily unanimity. Consensus requires that all views and objections be considered and that effort be made toward their resolution.

The use of American National Standards is completely voluntary; their existence does not in any respect preclude anyone, whether he or she has approved the standards or not, from manufacturing, marketing, purchasing, or using products, processes, or procedures not confirming to the standards.

The American National Standards Institute does not develop standards and will in no circumstances give interpretation on any American National Standard in the name of the American National Standards Institute. Requests for interpretations should be addressed to the secretariat or sponsor whose name appears on the title page of this standard.

CAUTION NOTICE: This American National Standard may be revised or withdrawn at any time. The procedures of the American National Standards Institute require that action be taken periodically to reaffirm, revise, or withdraw this standard. Purchasers of American National Standards may receive current information on all standards by calling or writing the American National Standards Institute.

CAUTION: The developers of this standard have requested that holders of patents that may be required for the implementation of the standard disclose such patents to the publisher. However, neither the developers nor the publisher have undertaken a patent search in order to identify which, if any, patents may apply to this standard.

As of the date of publication of this standard, following calls for the identification of patents that may be required for the implementation of the standard, notice of one or more such claims has been received.

By publication of this standard, no position is taken with respect to the validity of this claim or of any rights in connection therewith. The known patent holder(s) has (have), however, filed a statement of willingness to grant a license under these rights on reasonable and nondiscriminatory terms and conditions to applicants desiring to obtain such a license. Details may be obtained from the publisher.

No further patent search is conducted by the developer or publisher in respect to any standard it processes. No representation is made or implied that this is the only license that may be required to avoid infringement in the use of this standard.

Published by
American National Standards Institute
11 West 42nd Street, New York, NY 10036

Printed in the United States of America

Contents

Tables

Figures

Foreword

This foreword is not part of American National Standard INCITS.***:2007.

This standard specifies the external behavior of a device server that defines itself as an automation/drive interface device in the DEVICE TYPE field of the standard INQUIRY data. This device type is known as an automation/drive interface device.

With any technical document there may arise questions of interpretation as new products are implemented. INCITS has established procedures to issue technical opinions concerning the standards developed by INCITS. These procedures may result in SCSI Technical Information Bulletins being published by INCITS.

These Bulletins, while reflecting the opinion of the Technical Committee that developed the standard, are intended solely as supplementary information to other users of the standard. This standard, ANSI IINCITS.***:2007, as approved through the publication and voting procedures of the American National Standards Institute, is not altered by these bulletins. Any subsequent revision to this standard may or may not reflect the contents of these Technical Information Bulletins.

Current INCITS practice is to make Technical Information Bulletins available through:

INCITS Online Store	http://www.techstreet.com/INCITS.html
managed by Techstreet	Telephone: 1-734-302-7801 or
1327 Jones Drive	1-800-699-9277
Ann Arbor, MI 48105 Facsimile:	1-734-302-7811

or

IHS	http://global.ihs.com/
15 Inverness Way East	Telephone: 1-303-792-2181 or
Englewood, CO 80112-5704	1-800-854-7179
	Facsimile: 1-303-792-2192

Requests for interpretation, suggestions for improvement and addenda, or defect reports are welcome. They should be sent to the INCITS Secretariat, InterNational Committee for Information Technology Standards, Information Technology Institute, 1250 Eye Street, NW, Suite 200, Washington, DC 20005-3922.

This standard was processed and approved for submittal to ANSI by the InterNational Committee for Information Technology Standards (INCITS). Committee approval of the standard does not necessarily imply that all committee members voted for approval. At the time it approved this standard, INCITS had the following members:

(Editor’s Note: Insert INCITS member list)

Technical Committee T10 on SCSI Storage Interfaces, which developed and reviewed this standard, had the following members:

John B. Lohmeyer, Chair
Mark Evans, Vice-Chair
Ralph O. Weber, Secretary

Organization Represented	*Name of Representative*
AMCC	Paul von Stamwitz
Brocade	David Peterson
	Robert Snively (Alt)
Dell, Inc.	Kevin Marks
EMC Corp.	Gary S. Robinson
	David Black (Alt)
	Sean Dolan (Alt)
	Mickey Felton (Alt)
Emulex	William Martin
	Robert H. Nixon (Alt)
ENDL Texas	Ralph O. Weber
	I. Dal Allan (Alt)
FCI	Douglas Wagner
Finisar Corp.	David Freeman
	Chris Cicchetti (Alt)
	Paul Gentieu (Alt)
	Geoffrey Hibbert (Alt)
	Monica Li (Alt)
Foxconn Electronics	Elwood Parsons
Fujitsu	Mike Fitzpatrick
	Ben-Koon Lin (Alt)
General Dynamics	Nathan Hastad
	Tim Mackley (Alt)
Hewlett Packard Co.	Rob Elliott
	Curtis Ballard (Alt)
	Michael Banther (Alt)
	Wayne Bellamy (Alt)
	Steven Fairchild (Alt)
	Barry Olawsky (Alt)
	Christopher Williams (Alt)
	Jeff Wolford (Alt)
Hitachi Global Storage Tech.	Dan Colegrove
	Dan Reno (Alt)
IBM Corp.	Kevin Butt
	Ted Vojnovich (Alt)
Intel Corp.	Mark Seidel
Iomega Corp.	Robert Payne
Kawasaki Microelectronics Am	Joel Silverman
KnowledgeTek, Inc.	Dennis Moore
Lexar Media, Inc.	John Geldman

LSI Corp.	John Lohmeyer
	Brad Besmer (Alt)
	Brian Day (Alt)
	Keith Holt (Alt)
	Walt Hubis (Alt)
	Michael Jenkins (Alt)
	Steve Johnson (Alt)
	Dennis Kleppen (Alt)
	Bernhard Laschinsky (Alt)
	George Penokie (Alt)
	Robert Sheffield (Alt)
Marvell Semiconductor, Inc.	David Geddes
	Jacky Chow (Alt)
	Paul Wassenberg (Alt)
Maxim Integrated Products	Gregory Tabor
	David Allen (Alt)
	Mahbubul Bari (Alt)
Microsoft Corp.	Mark Benedikt
	Robert Griswold (Alt)
Molex Inc.	Jay Neer
	Galen Fromm (Alt)
NetApp	Frederick Knight
	Chris Fore (Alt)
	Subhash Sankuratripati (Alt)
Nvidia Corp.	Mark Overby
	Andrew Currid (Alt)
PMC-Sierra	Tim Symons
	Guillaume Fortin (Alt)
	Mathieu Gagnon (Alt)
	Rick Hernandez (Alt)
Quantum Corp.	Paul Suhler
	Paul Stone (Alt)
	Rod Wideman (Alt)
Samsung	Joseph Chen
	Edward Chang (Alt)
	Sung H. Lee (Alt)
	Dmitry Obukhov (Alt)
SanDisk Corporation	Avraham Shimor
	Dave Landsman (Alt)
	Donald Rich (Alt)
	Yoni Shternhell (Alt)
Seagate Technology	Gerald Houlder
	Alvin Cox (Alt)
	Jim Hatfield (Alt)
STMicroelectonics, Inc.	Benoit MERCIER
Sun Microsystems, Inc.	Dale LaFollette
	Jon Allen (Alt)
	Vit Novak (Alt)
	Scott Painter (Alt)
Symantec	Roger Cummings
	Raymond Gilson (Alt)

TycoElectronics	Michael Fogg
	Ashlie Fan (Alt)
	Dan Gorenc (Alt)
	Scott Shuey (Alt)
	Robert Wertz (Alt)
Western Digital	Mark Evans
	Michael Rogers (Alt)
	Curtis Stevens (Alt)

Introduction

This standard is divided into the following clauses:

Clause 1 is the scope.
Clause 2 enumerates the normative references that apply to this standard.
Clause 3 describes the definitions, symbols, abbreviations, and conventions used in this standard.
Clause 4 describes an overview and model of the automation/drive interface device.
Clause 5 describes the command set for automation/drive interface devices.
Clause 6 describes the parameters for automation/drive interface devices.

American National Standard **INCITS.***:2008**

American National Standard for Information Systems - Information Technology - Automation/Drive Interface Commands - 3(ADC - 3)

1 Scope

This standard defines the model and command set extensions to facilitate operation of automation/drive interface devices. The clauses of this standard, implemented in conjunction with the applicable clauses of SPC-3, fully specifies the standard command set for automation/drive interface devices.

The objective of this standard is to provide the following:

a) permit an application client to communicate over a SCSI service delivery subsystem, with a logical unit that declares itself to be an automation/drive interface device in the PERIPHERAL DEVICE TYPE field of the standard INQUIRY data (see SPC-3);
b) define commands unique to the automation/drive interface device type; and
c) define commands and parameters to manage the operation of the automation/drive interface device type and the operation of logical units of other specific device types that are present in the same device as the automation/drive interface logical unit.

The following commands, parameter data, and features defined in previous versions of this standard are made obsolete by this standard: Linked commands.

Figure 1 shows the relationship of this standard to the other standards and related projects in the SCSI family standards as of the publication of this standard.

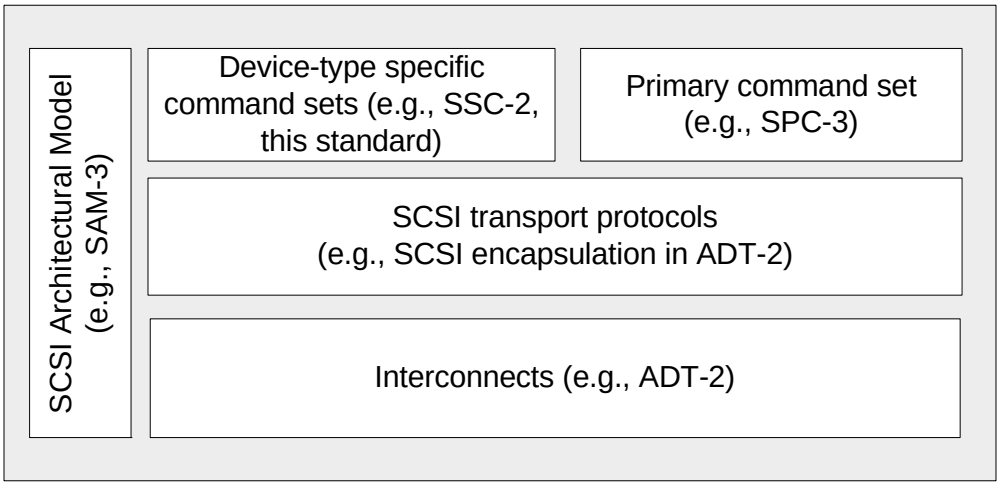

Figure 1 — General Document Structure of SCSI

Figure 1 is intended to show the general relationship of the documents to one another. Figure 1 is not intended to imply a relationship such as a hierarchy, protocol stack, or system architecture. It indicates the applicability of a standard to the implementation of a given transport.

Commands in this standard do not require the use of a specific SCSI transport protocol.

2 Normative References

2.1 Normative references overview

The following standards contain provisions that, by reference in the text, constitute provisions of this standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this standard are encouraged to investigate the possibility of applying the most recent editions of the standards listed below.

Copies of the following documents may be obtained from ANSI: approved ANSI standards, approved and draft international and regional standards (ISO, IEC, CEN/CENELEC, ITUT), and approved and draft foreign standards (including BSI, JIS, and DIN). For further information, contact ANSI Customer Service Department at 212-642-4900 (phone), 212-302-1286 (fax) or via the World Wide Web at http://www.ansi.org.

Additional availability contact information is provided below as needed.

2.2 Approved references

ISO/IEC 14776-412, *SCSI Architecture Model - 2* (SAM-2) [ANSI INCITS 366-2003]

ISO/IEC 14776-413, *SCSI Architecture Model - 3* (SAM-3) [ANSI INCITS 402-2005]

ISO/IEC 14776-452, *SCSI Primary Commands - 2* (SPC-2) [ANSI INCITS 351-2001]

ISO/IEC 14776-453, *SCSI Primary Commands - 3* (SPC-3) [ANSI INCITS 408-2005]

ISO/IEC 14776-332, *SCSI Stream Commands - 2* (SSC-2) [ANSI INCITS 380-2003]

ISO/IEC 14776-352, *SCSI Media Changer Commands - 2* (SMC-2) [ANSI INCITS 382-2004]

ISO/IEC 14776-364, *Multimedia Commands - 4* (MMC-4) [ANSI INCITS 401-2005]

ISO/IEC 14165-251, *Fibre Channel Framing and Signaling Interface* (FC-FS) [ANSI INCITS 373-2003]

ISO/IEC 14165-122, *Fibre Channel Arbitrated Loop - 2* (FC-AL-2) [ANSI INCITS 332-1999]

ISO/IEC 14776-223, *SCSI Fibre Channel Protocol - 3* (FCP-3) [ANSI INCITS 416-2006]

ISO/IEC 14776-115, *SCSI Parallel Interface - 5* (SPI-5) [ANSI INCITS 367-2003]

ISO/IEC 14776-151, *Serial Attached SCSI - 1.1* (SAS-1.1) [ANSI INCITS 417-2006]

ISO/IEC 14776-191, *Automation/Drive Interface, Transport Protocol* (ADT) [ANSI INCITS 406-2005]

2.3 References under development

At the time of publication, the following referenced standards were still under development. For information on the current status of the document, or regarding availability, contact the relevant standards body or other organization as indicated.

ISO/IEC 14776-414, SCSI Architecture Model - 4 (SAM-4) [T10/1683-D]

ISO/IEC 14776-454, *SCSI Primary Commands - 4* (SPC-4) [T10/1731-D]

ISO/IEC 14776-333, *SCSI Stream Commands - 3* (SSC-3) [T10/1611-D]

ISO/IEC 14776-352, *SCSI Media Changer Commands - 3* (SMC-3) [T10/1730-D]

ISO/IEC 14776-192, *Automation/Drive Interface, Transport Protocol - 2* (ADT-2). [T10/1742-D]

3 Definitions, symbols, abbreviations, and conventions

3.1 Definitions

3.1.1 accessible state: The state of a device server in which it is capable of responding to a command with any combination other than CHECK CONDITION status with the sense key set to NOT READY.

3.1.2 ADC device server: A device server (see 3.1.17) that reports the value 12h in the PERIPHERAL DEVICE TYPE field of its standard INQUIRY data (see SPC-3).

3.1.3 ADC logical unit: A logical unit (see 3.1.24) containing an ADC device server (see 3.1.2).

3.1.4 ADI port: A port used to connect an automation device (see 3.1.9) and a DT device (see 3.1.15), that is not a DT device primary port (see 3.1.16) and not an automation device primary port (see 3.1.10). It supports a transport protocol that passes SCSI requests and SCSI responses (e.g., ADT or USB).

3.1.5 additional sense data: The combination of values in an ASC field and an ASCQ field (see 5.2).

3.1.6 ADT port: An ADI port that implements ADT.

3.1.7 application client: An object that is the source of commands and task management function requests (see SAM-3).

3.1.8 automation application client: In an automation device, the application client of the ADC device server in the DT device (see 4.1).

3.1.9 automation device: A device containing one or more SMC device servers (see SMC-2) or equivalent, one or more automation application clients, and one or more ports to access a DT device (e.g., an ADI port). An automation device may contain one or more automation device primary ports (see 4.1).

3.1.10 automation device primary port: A SCSI target port or a SCSI target/initiator port (see SAM-3) in an automation device (see 3.1.9).

3.1.11 bridging: A DT device (see 3.1.15) facilitating invocation of commands or task management requests on the remote SMC logical unit (see 4.3).

3.1.12 bridging manager: In a DT device implementing bridging (see 4.3), the application client of the remote SMC device server (see 3.1.34).

3.1.13 byte: A sequence of eight contiguous bits considered as a unit.

3.1.14 contingent allegiance: An optional condition of a task set following the return of a CHECK CONDITION status (see SAM-2).

3.1.15 data transfer (DT) device: A device containing an RMC device server, an ADC device server, one or more ports to access an automation device (e.g., an ADI port), and one or more DT device primary ports (see 4.1). A data transfer device may contain a bridging manager and local SMC device server (see 4.3).

3.1.16 data transfer (DT) device primary port: A SCSI target port in a data transfer device (see 3.1.15).

3.1.17 device server: An object within the logical unit that processes SCSI tasks according to the rules for task management (see SAM-3).

3.1.18 DT device management interface: An interface outside the scope of this standard that allows configuration and control of a DT device.

3.1.19 field: A group of one or more contiguous bits.

3.1.20 I_T nexus: A nexus that exists between a SCSI initiator port and a SCSI target port (see SAM-3).

3.1.21 I_T_L nexus: A nexus that exists between a SCSI initiator port, a SCSI target port, and a logical unit (see SAM-3). This relationship extends the prior I_T nexus.

3.1.22 local SMC device server: The SMC device server in a DT device implementing bridging (see 4.3).

3.1.23 local SMC logical unit: An SMC logical unit (see 3.1.45) in a DT device containing a local SMC device server (see 3.1.22).

3.1.24 logical unit: A SCSI target device object, containing a device server and task manager, that implements a device model and manages tasks to process commands sent by an application client (see SAM-3).

3.1.25 logical unit number (LUN): An identifier for a logical unit.

3.1.26 logical unit reset: A logical unit action in response to a logical unit reset event in which the logical unit performs the operations described in SAM-3.

3.1.27 logical unit reset event: An event that triggers a logical unit reset from a logical unit (see SAM-3).

3.1.28 medium: The operational substrate and its carrier that is removable from a DT device.

3.1.29 nexus: A relationship between two SCSI devices, and the SCSI initiator port and SCSI target port objects within those SCSI devices.

3.1.30 not accessible state: The state of a device server in which it is only capable of responding to a command with CHECK CONDITION status with the sense key set to NOT READY.

3.1.31 object: An architectural abstraction that encapsulates data types, services, or other objects that are related in some way.

3.1.32 physical device: An object in a SCSI target device that performs operations on a medium (e.g., reading, writing, loading, and unloading). See SSC-3.

3.1.33 ready state: A state where a logical unit is able to process a medium-access command without returning CHECK CONDITION status with the sense key set to NOT READY.

3.1.34 remote SMC device server: The SMC device server in an automation device that receives commands via a DT device implementing bridging (see 4.3).

3.1.35 remote SMC logical unit: An SMC logical unit (see 3.1.45) in an automation device containing a remote SMC device server (see 3.1.34).

3.1.36 removable medium commands (RMC): A generic term for a command set supporting removable media (e.g., SSC-2 or MMC-4).

3.1.37 RMC device server: A device server (see 3.1.17) that supports removable medium commands (see 3.1.36).

3.1.38 RMC logical unit: A logical unit (see 3.1.24) containing an RMC device server (see 3.1.37).

3.1.39 SCSI initiator device: A SCSI device containing application clients and SCSI initiator ports that originates device service and task management requests to be processed by a SCSI target device and receives device service and task management responses from SCSI target devices. When used this term refers to SCSI initiator devices or SCSI target/initiator devices that are using the SCSI target/initiator port as a SCSI initiator port (see SAM-3).

3.1.40 SCSI initiator port: A SCSI initiator device object that acts as the connection between application clients and the service delivery subsystem through which requests, indications, responses, and confirmations are routed. In all cases when this term is used it refers to an initiator port or a SCSI target/initiator port operating as a SCSI initiator port (see SAM-3).

3.1.41 SCSI target device: A SCSI device containing logical units and SCSI target ports that receives device service and task management requests for processing and sends device service and task management responses to SCSI initiator devices. When used this term refers to SCSI target devices or SCSI target/initiator devices that are using the SCSI target/initiator port as a SCSI target port (see SAM-3).

3.1.42 SCSI target port: A SCSI target device object that contains a task router and acts as the connection between device servers and task managers and the service delivery subsystem through which indications and responses are routed. When this term is used it refers to a SCSI target port or a SCSI target/initiator port operating as a SCSI target port (see SAM-3).

3.1.43 sense masking timeout value (SM_TOV): A period of time for which a DT device masks sense data (see 4.5).

3.1.44 SMC device server: A device server (see 3.1.17) that reports the value 08h in the PERIPHERAL DEVICE TYPE field of its standard INQUIRY data (see SPC-3).

3.1.45 SMC logical unit: A logical unit (see 3.1.24) containing an SMC device server (see 3.1.44).

3.1.46 storage element: A component of a medium changer device used only for storage of a medium (see SMC-2).

3.1.47 task: An object within the logical unit representing the work associated with a command. A task consists of one initial connection and zero or more physical or logical reconnections, all pertaining to the task.

3.1.48 task management request: A request that a task management function be performed (see SAM-3).

3.1.49 task set: A group of tasks within a logical unit (see 3.1.24), whose interaction is dependent on the task management and auto-contingent allegiance rules (see SAM-3) and the contingent allegiance rules (see SAM-2).

3.1.50 vendor-specific (VS): Something (e.g., a bit, field, code value) that is not defined by this standard and may be used differently in various implementations.

3.1.51 zero: A false signal value or a false condition of a variable.

3.2 Symbols and abbreviations

= or EQ	equal
ADC	Automation/Drive Interface - Commands
ADC-2	Automation/Drive Interface - Commands - 2

ADC-3	Automation/Drive Interface - Commands - 3
ADI	Automation/Drive Interface
ADT	Automation/Drive Interface - Transport Protocol
ADT-2	Automation/Drive Interface - Transport Protocol - 2
DT	data transfer (e.g., DT device)
FC-AL-2	Fibre Channel Arbitrated Loop (see 2)
FC-FS	Fibre Channel Framing and Signaling (see 2)
FCP-3	Fibre Channel Protocol-3
Gb/sec	gigabits per second
LSB	least significant bit
LUN	logical unit number
MAM	medium auxiliary memory (see SPC-3)
MSB	most significant bit
MMC-4	Multimedia Commands - 4
RMC	removable medium commands (see 3.1.36)
Rsvd	reserved
SAM-2	SCSI Architecture Model - 2
SAM-3	SCSI Architecture Model - 3
SAS-1.1	Serial Attached SCSI - 1.1
SCSI	Small Computer System Interface
SM_TOV	sense masking timeout value (see 4.5)
SMC	SCSI Media Changer Commands
SMC-2	SCSI Media Changer Commands - 2
SMC-3	SCSI Media Changer Commands - 3
SPC-2	SCSI Primary Commands - 2
SPC-3	SCSI Primary Commands - 3
SPC-4	SCSI Primary Commands - 4
SPI-5	SCSI Parallel Interface - 5 (see 2)
SSC	SCSI Stream Commands
SSC-2	SCSI Stream Commands - 2
SSC-3	SCSI Stream Commands - 3
VHF	very high frequency (e.g., VHF data)
VPD	vital product data (see SPC-3)
VS	vendor-specific (see 3.1.50)

3.3 Keywords

3.3.1 invalid: A keyword used to describe an illegal or unsupported bit, byte, word, field or code value. Receipt of an invalid bit, byte, word, field or code value shall be reported as an error.

3.3.2 mandatory: A keyword indicating an item that is required to be implemented as defined in this standard to claim compliance with this standard.

3.3.3 may: A keyword that indicates flexibility of choice with no implied preference.

3.3.4 may not: Keywords that indicate flexibility of choice with no implied preference.

3.3.5 obsolete: A keyword indicating that an item was defined in prior SCSI standards but has been removed from this standard.

3.3.6 optional: A keyword that describes features that are not required to be implemented by this standard. However, if any optional feature defined by this standards is implemented, then it shall be implemented as defined in this standard.

3.3.7 reserved: A keyword referring to bits, bytes, words, fields and code values that are set aside for future standardization. Their use and interpretation may be specified by future extensions to this or other standards. A reserved bit, byte, word or field shall be set to zero, or in accordance with a future extension to this standard. Recipients are not required to check reserved bits, bytes, words or fields for zero values. Receipt of reserved code values in defined fields shall be reported as an error.

3.3.8 shall: A keyword indicating a mandatory requirement. Designers are required to implement all such requirements to ensure interpoperability with other products that conform to this standard.

3.3.9 should: A keyword indicating flexibility of choice with a preferred alternative; equivalent to the phrase "it is recommended."

3.4 Conventions

Certain words and terms used in this American National Standard have a specific meaning beyond the normal English meaning. These words and terms are defined either in clause 3 or in the text where they first appear. Names of signals, phases, messages, commands, statuses, sense keys, additional sense codes, and additional sense code qualifiers are in all uppercase (e.g., REQUEST SENSE), names of fields are in small uppercase (e.g., PARAMETER LIST LENGTH), lower case is used for words having the normal English meaning.

Fields containing only one bit are usually referred to as the name bit instead of the name field.

A binary number is represented in this standard by any sequence of digits comprised of only the Western-Arabic numerals 0 and 1 immediately followed by a lower-case b (e.g., 0101b). Underscores or spaces may be included in binary number representations to increase readability or delineate field boundaries (e.g., 0 0101 1010b or 0_0101_1010b).

A hexadecimal number is represented in this standard by any sequence of digits comprised of only the Western-Arabic numerals 0 through 9 and/or the upper-case English letters A through F immediately followed by a lower-case h (e.g., FA23h). Underscores or spaces may be included in hexadecimal number representations to increase readability or delineate field boundaries (e.g., B FD8C FA23h or B_FD8C_FA23h).

A decimal number is represented in this standard by any sequence of digits comprised of only the Western-Arabic numerals 0 through 9 not immediately followed by a lower-case b or lower-case h (e.g., 25).

When the value of the bit or field is not relevant, x or xx appears in place of a specific value.

This standard uses the ISO convention for representing decimal numbers (e.g., the thousands and higher multiples are separated by a space and a comma is used as the decimal point). Table 1 shows some examples of decimal numbers represented using the ISO and American conventions.

Table 1 — ISO and American numbering conventions examples

ISO	American
0,6	0.6
3,141 592 65	3.14159265
1 000	1, 000
1 323 462,95	1,323,462.95

Lists sequenced by letters (e.g., a-red, b-blue, c-green) show no priority relationship between the listed items. Numbered lists (e.g., 1-red, 2-blue, 3-green) show a priority ordering between the listed items.

If a conflict arises between text, tables, or figures, the order of precedence to resolve the conflicts is text; then tables; and finally figures. Not all tables or figures are fully described in the text. Tables show data format and values.

Notes and examples do not constitute any requirements for implementors.

4 General

4.1 Automation/drive interface model overview

An Automation/Drive Interface Commands - 3 (ADC-3) device server provides the means for an automation device (e.g., a media changer) to monitor and control a data transfer (DT) device (e.g., a removable medium device such as a tape drive).

An automation device contains:

a) an SMC logical unit, which controls a mechanism to move storage media among DT devices and storage elements;
b) zero or more automation device primary ports, through which the SMC logical unit receives SCSI commands or task management requests;
c) an automation application client (see 3.1.8); and
d) one or more ports through which the automation application client transmits SCSI requests to and receives SCSI responses from the ADC device server in the DT device.

A DT device contains:

a) an ADC device server;
b) an RMC device server (e.g., an SSC device server), which processes tasks from application clients performing write and read operations;
c) an optional SMC device server and corresponding bridging manager (see 4.3); and
d) one or more ports through which the device servers and bridging manager contained within the DT device pass SCSI requests and SCSI responses. At least one of these ports shall be a DT device primary port (see 3.1.16). One of these ports may be an ADI port (see 3.1.4).

The automation application client may perform one or more of the following operations:

a) configure the DT device's operational parameters (e.g., SCSI Port ID, Fibre Channel target device name, and Autoload mode);
b) enable or disable the DT device primary ports (e.g., Parallel SCSI or Fibre Channel);
c) determine the DT device's status, including the position of the removable medium and whether a medium access command is in process; or
d) cause the DT device to unload or load a medium, even if its RMC device server is reserved by an application client (see 4.2).

These operations are performed by invoking various commands and task management requests on the ADC logical unit. The application client within the automation device that invokes these requests is called the automation application client. Communication between device servers within the automation device and the automation application client are outside the scope of this standard.

Figure 2 shows an example hardware view of the relationship between an automation device and DT devices using ADT transport protocol interfaces.

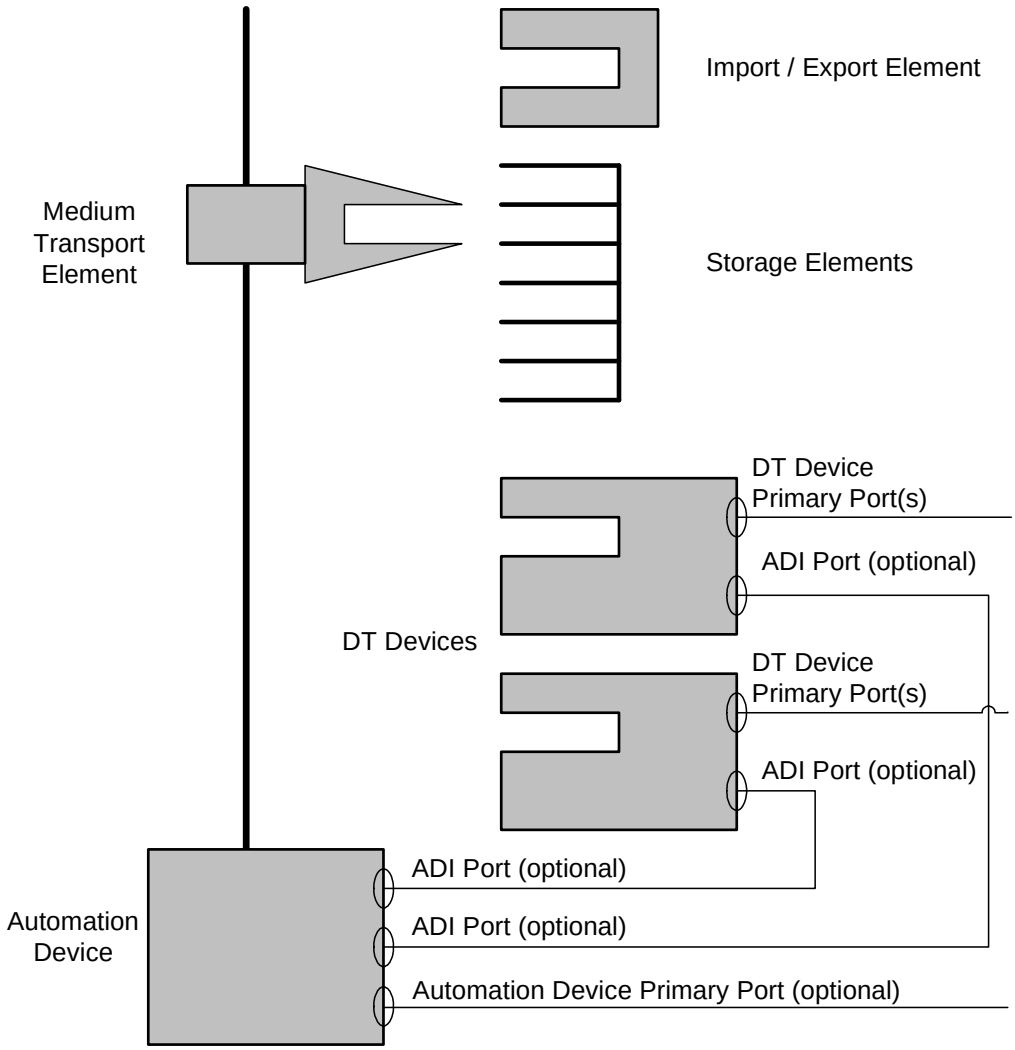

Figure 2 — Example of an automation device and DT device relationship

4.2 Device server interaction

Figure 3 shows:

a) an automation device with an automation application client and a remote SMC device server; and
b) a DT device with an RMC device server, an ADC device server, and an optional local SMC device server (see 4.3).

Because the RMC and ADC device servers coexist within a single target device and serve the same physical device, they interact with each other in various ways.

If enabled (see 6.2.2.3.2), then the RMC device server shall be accessible as a logical unit through a DT device primary port. If the DT device contains an ADI port, then the RMC device server should be accessible as a logical unit through an ADI port, and may support asymmetric logical unit access (see SPC-3).

The ADC device server may be accessible as a logical unit through a DT device primary port. If the DT device does not contain an ADI port, then the ADC device server shall be accessible as a logical unit through a DT device primary port. If the DT device contains an ADI port, then the ADC device server shall be accessible as a logical unit through an ADI port.

PREVENT ALLOW MEDIUM REMOVAL commands (see SPC-3) issued to the RMC device server shall not affect the ADC device server.

Sense data reported by the RMC device server may be masked (see 4.5) for a period of time while the automation device is in the process of loading a medium. The NOTIFY DATA TRANSFER DEVICE command (see 5.2) provides a mechanism for the automation application client to indicate that the load attempt has ended in a failure and the RMC device server that was masking sense data changes shall resume reporting sense data for the failure.

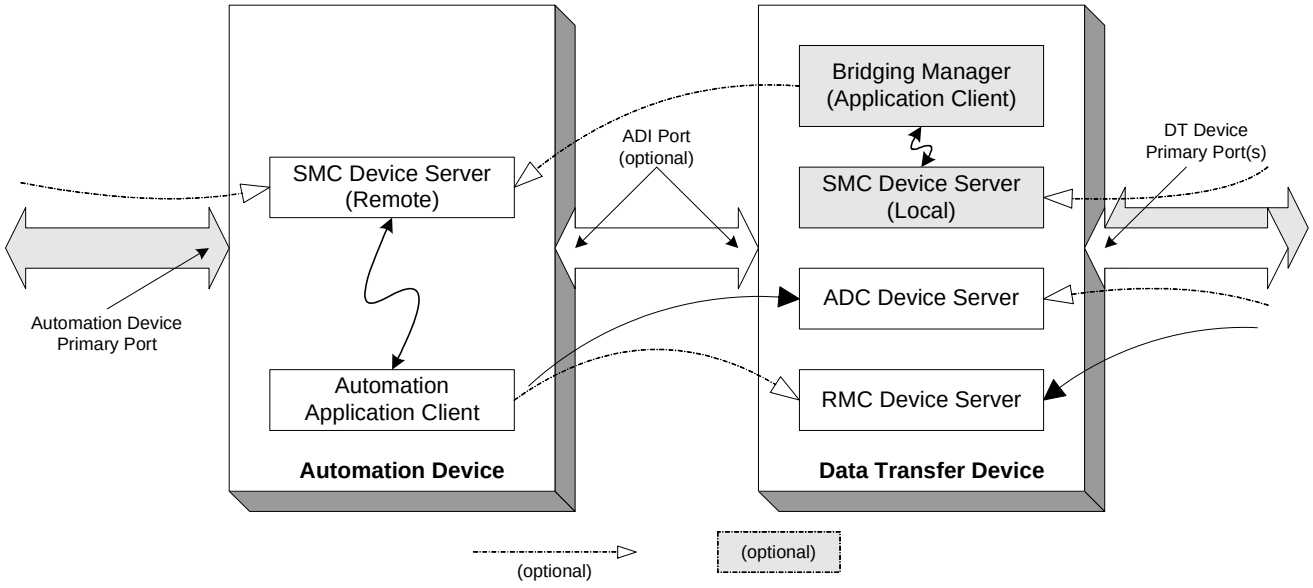

Figure 3 — Device server model

Since the RMC and ADC device servers share the same physical device, operations related to the physical device are cause for interaction between the RMC and ADC device servers. Unit attention conditions shall be established by both the RMC and ADC device servers for causes based on the shared physical device (e.g., pressing an eject button on the physical device). Unit attention conditions shall not be propagated across both the RMC and ADC device servers for causes that are strictly within the domain of one device server.

The ADC device server shall not support reservations. The ADC device server avoids reservation conflicts with other device servers since reservations held against one device server do not affect other device servers.

NOTE 1 This approach allows the automation application client to interact with the physical device via the ADC device server without a conflict due to reservations on other device servers.

The ADC device server supports mode pages that affect the RMC device server (see 6.2.2.3.2). The ADC mode pages override some mode parameters of the RMC device server (e.g., load or unload behavior).

Some commands supported by the ADC device server are dependent upon the readiness of the removable medium (see table 7). The response to a TEST UNIT READY command (see SPC-3) issued to the ADC device

server indicates the readiness of the removable medium. The ADC device server shall establish a unit attention condition with an additional sense code of NOT READY TO READY CHANGE, MEDIUM MAY HAVE CHANGED based on the transition from not ready to ready of the removable medium.

A LOAD UNLOAD command (see SSC-2) processed by the ADC device server may affect the ready state (see 3.1.33) of the RMC device server and shall cause the RMC device server to establish appropriate unit attention condition. A LOAD UNLOAD command processed by the RMC device server may affect the ready state of the ADC device server and shall cause the ADC device server to establish appropriate unit attention condition. The interaction between the ADC task set and other task sets within the DT device are vendor-specific.

The RMC and ADC device servers maintain independent TapeAlert flags (see 4.6) and return them to application clients. Retrieving the TapeAlert flag information from the ADC device server has no impact on the TapeAlert flags reported by the RMC device server. Retrieving the TapeAlert flag information from the RMC device server has no impact on the TapeAlert flags reported by the ADC device server.

Communication between the application clients and device servers within a DT device, and application clients and device servers and the DT device itself are outside the scope of this standard.

4.3 ADI bridging

4.3.1 ADI bridging introduction

The DT device may support ADI bridging for the automation device. When ADI bridging is enabled via the ENABLE bit of the SMC Logical Unit descriptor (see 6.2.2.3.3), the DT device shall contain the bridging manager and the local SMC device server (see figure 3). The DT device shall report to its DT device primary port(s) a local SMC logical unit (see 3.1.23), and the automation device shall report a remote SMC logical unit (see 3.1.35) to the automation device ADI port. The local SMC logical unit may be accessible through the DT device ADI port, and may support asymmetric logical unit access (see SPC-3).

The local SMC logical unit receives a command or task management request via a DT device primary port. In processing the command or task management request, the local SMC logical unit may require the automation device to perform additional processing. To perform this addition processing, the local SMC logical unit passes requests to an application client in the DT device (i.e., the bridging manager). This communication is performed by means outside the scope of this standard. Using the ADI ports on the DT device and automation device, the bridging manager then invokes commands or task management requests on the remote SMC logical unit that resides in the automation device.

As a result some or all commands and task management requests addressed to the local SMC logical unit are passed to the remote SMC logical unit through the ADI port.

4.3.2 Local SMC device server operation

ADI bridging is enabled and disabled via the SMC Logical Unit descriptor of the ADC Device Server Configuration mode page implemented by the ADC device server (see 6.2.2.3.3). The descriptor specifies the logical unit number of the corresponding local SMC device server. When bridging is disabled, the SMC logical unit shall not be included in the logical unit inventory (see SPC-3) and shall be considered an incorrect logical unit by the task routers (see SAM-3).

The local SMC device server shall support commands as required by the SCSI Media changer device type. If the transport protocol connecting the bridging manager and the remote SMC logical unit does not carry information about which I_T nexus originated a SCSI command or task management request, then the remote SMC device

server is not able to implement the complete set of commands. As a result, the local SMC logical unit shall service commands and task management functions that require knowledge of the originating initiator port.

If any of the following commands are supported, then they shall be processed by the local SMC device server and not passed through to the remote SMC device server:

a) RESERVE(6) and RESERVE(10) (see SPC-2);
b) RELEASE(6) and RELEASE(10) (see SPC-2);
c) PERSISTENT RESERVE IN (see SPC-3);
d) PERSISTENT RESERVE OUT (see SPC-3);
e) REPORT LUNS (see SPC-3); or
f) REQUEST SENSE (see SPC-3).

The local SMC device server shall not support element reservations in the RESERVE(6), RELEASE(6), RESERVE(10), and RELEASE(10) commands.

The local SMC device server shall also perform the following actions:

a) check for reservation conflicts on all commands and return RESERVATION CONFLICT status on all commands that violate reservation rules (see SPC-3);
b) manage unit attention conditions established for multiple initiator ports. If the local SMC device server detects that a unit attention condition is pending for an initiator port when a new command is received, the local SMC device server shall return CHECK CONDITION status for the command; and
c) save sense data on a per I_T nexus basis, if a DT device primary port uses contingent allegiance (see SAM-2).

The local SMC device server may augment information returned by the remote SMC device server based on information known only by the local SMC device server (e.g., Device Identification VPD page identification descriptors with an ASSOCIATION FIELD set to 01b (i.e., target port) and supported operation codes).

The local SMC device server may process the following commands without passing them through to the remote SMC device server:

a) REPORT SUPPORTED OPERATION CODES (see SPC-3); and
b) REPORT SUPPORTED TASK MANAGEMENT FUNCTIONS (see SPC-3).

4.3.3 Remote SMC device server operation

The remote SMC device server shall not support any protocol-specific mode pages or protocol-specific log pages.

The remote SMC device server shall not report Device Identification VPD page identification descriptors with an ASSOCIATION FIELD set to 01b (i.e., target port).

The automation application client shall report all unit attention conditions established in the remote SMC device server for all initiator ports to the ADC device server using the NOTIFY DATA TRANSFER DEVICE command (see 5.2).

4.3.4 Bridging manager operation

ADI bridging is enabled and disabled via the SMC Logical Unit descriptor of the ADC Device Server Configuration mode page implemented by the ADC device server (see 6.2.2.3.3). The descriptor specifies the logical unit number of the corresponding remote SMC device server.

If the bridging manager receives a response from the remote SMC device server with a CHECK CONDITION status with the sense key set to UNIT ATTENTION, then the bridging manager shall discard the response and reissue the command. All other responses with a status of CHECK CONDITION, including those with a sense key of NOT READY, shall be returned to the local SMC device server.

After issuing a command to the remote SMC device server, the bridging manager shall not issue another command to the remote SMC device server until the previous command completes or is aborted.

4.3.5 Caching SMC data and status

The local SMC device server may preserve some data or status received from the remote SMC device server in a cache, in order to respond to certain commands without need for the bridging manager to invoke a command on the remote SMC device server (e.g., the local SMC device server may save the standard INQUIRY data from the remote SMC device server and return the data to any initiator port that requests it). The local SMC device server shall invalidate any data and status previously saved in a cache if the ENABLE bit in the SMC Logical Unit descriptor (see 6.2.2.3.3) is set to zero or the CACHE bit in the SMC Logical Unit descriptor is set to zero.

Caching of SMC ready state, standard INQUIRY data (see SPC-3), VPD data, mode data, and supported operation codes is controlled by the CACHE bit in the SMC Logical Unit descriptor (see 6.2.2.3.3). When the CACHE bit is set to one, caching is enabled. If caching is enabled, then the automation application client shall send the NOTIFY DATA TRANSFER DEVICE command (see 5.2) to the ADC device server when events occur that may change data cached by the local SMC device server. When the local SMC device server detects a possible change in the cached data, the local SMC device server shall discontinue using the cached data until the cached data has been updated. An ADC device server that supports setting the CACHE bit to one in the SMC Logical Unit descriptor shall also support a NOTIFY DATA TRANSFER DEVICE command with a value of one in one or more of the MDC bit, IDC bit, NRSC bit, and SOCC bit (see 5.2).

If caching is disabled, then the ADC device server shall ignore the MDC bit, IDC bit, NRSC bit, and socc bit in the NOTIFY DATA TRANSFER DEVICE command. As a result, the automation application client is not required to send a NOTIFY DATA TRANSFER DEVICE command for purposes of indicating changes in cached data. The automation application client may send a NOTIFY DATA TRANSFER DEVICE command to notify the ADC device server of events not related to changes in cached data.

Ready state indicates whether the remote SMC device server is accessible. The remote SMC device server is not accessible if it would respond to a command with a CHECK CONDITION status with the sense key set to NOT READY. Otherwise, it is accessible. The local SMC device server may monitor the ready state of the remote SMC device server via the cache. If the ready state indicates not accessible, then the local SMC device server shall terminate commands that require the remote SMC device server to be accessible (see SMC-3) with CHECK CONDITION status, with the sense key to NOT READY, and the additional sense code set to the additional sense code contained in the cache.

4.4 Load and unload states

4.4.1 Load states

Table 2 defines the states that may be reported in the VHF data descriptor (see 6.1.2.2) during load operations. This information allows automation devices to coordinate loading and unloading of a medium with the DT device, and to obtain DT device activity status.

Table 2 — Load states

Load state	Bit in the VHF data descriptor					
	INXTN	RAA	MPRSNT	MSTD	MTHRD	MOUNTED
a) DT device initialized, no medium present	0	1	0	0	0	0
b) Early detection of medium placement by DT device	0	1	1	0	0	0
c) Acknowledgement of medium control by DT device	0	0	1	0	0	0
d) Medium seating	1	0	1	0	0	0
e) Medium seated	0	0	1	1	0	0
f) Medium threading	1	0	1	1	0	0
g) Medium threaded	0	0	1	1	1	0
h) Completing load	1	0	1	1	1	0
i) Medium mounted	0	0	1	1	1	1

Load states (a) and (i) shall be supported by the ADC device server. States (b) through (h) (i.e., all other states) should be supported to accurately reflect the states used by the DT device. Load states may not be reported in the order listed in table 2.

To indicate an error in any of the listed states, or to report a state not listed, the RRQST bit in the VHF data descriptor shall be set to one and the INXTN bit shall be set to zero.

The DT device shall set the INXTN bit to zero when the DT device requires an external stimulus (e.g., a command or medium movement) to attempt to reach another state. The DT device may set the INXTN bit to zero when the DT device requires an internal stimulus (e.g., completion of a cleaning operation when using a cleaning cartridge) to attempt to reach another state.

Load state (a) represents an empty DT device, available for loading by the automation device.

Load state (b) represents initial placement of a medium into the DT device by the automation device. Depending on the DT device's design, medium present may also be detected and reported coincident with load state (b). An additional external stimulus is required to leave load state (b) (e.g., medium movement caused by the automation device).

Load state (c) represents detection and acknowledgement by the DT device of medium presence, and that the DT device may now assume control of the medium and that the automation device should relinquish control of robotic access (e.g., this state may be reflected after medium movement caused by the automation device). An additional external stimulus is required to leave load state (c) (e.g., a LOAD UNLOAD command (see SSC-2) from the automation device).

Load state (d) represents a medium loading under the control of the DT device (e.g., to seat the medium).

Load state (e) represents a seated medium. An additional external stimulus is required to leave load state (e) (e.g., a command from the automation device or a LOAD UNLOAD command to the RMC device server). Load state (e) may be used in conjunction with MAM access.

Load state (f) represents a medium threading under control of the DT device.

Load state (g) represents a threaded medium. An additional external stimulus is required to leave load state (g) (e.g., a command from the automation device).

Load state (h) represents any additional processing that may be done by the DT device after threading the medium, but prior to the load being fully complete (e.g., allow data access).

Load state (i) represents a mounted medium.

A medium is mounted in a DT device when the DT device is physically capable of processing operations that involve interactions between the read/write element(s) of the DT device and the operational substrate of the medium. The interactions between the read/write element(s) of the DT device and the operational substrate of the medium may vary depending on the medium type (e.g., altering or detecting the magnetic polarization of the operational substrate for a magnetically recordable medium or physical abrasion of the read/write element(s) for a cleaning medium). A medium in a DT device is not mounted when the medium is seating, threading, positioning to its usable area, unthreading, or unseating. During operations involving a cleaning medium, some removable medium devices position to a previously unused location on the medium prior to performing the cleaning operation. For such technologies the device server should consider the medium as mounted prior to positioning over the previously used locations on the cleaning medium.

An example showing use of a few of the states is given in table 3.

Table 3 — Load states example

Load event	Bit in the VHF data descriptor					
	INXTN	RAA	MPRSNT	MSTD	MTHRD	MOUNTED
1) DT device initialized, no medium present	0	1	0	0	0	0
2) Initial medium placement into DT device	0	1	0	0	0	0
3) After the automation device pushes a medium into DT device, now seating	1	0	1	0	0	0
4) After seating, medium now threading	1	0	1	1	0	0
5) Medium threaded, completing load	1	0	1	1	1	0
6) Medium mounted	0	0	1	1	1	1

In this example, the DT device is loaded by the automation device first placing a medium into the DT device, then pushing the medium far enough into the DT device so that the DT device engages the medium and completes the operation in one continuous motion.

1) the load sequence begins with the DT device initialized, no medium present and robotic access allowed;
2) the automation device then places the medium into the DT device, which is not yet recognized by the DT device;

3) after the initial placement, the automation device pushes the medium into the DT device, such that medium presence is detected and the DT device assumes control of the medium and seats it;
4) the DT device continues transitioning through states as it threads the medium;
5) after threading, the DT device makes final microcode preparations to access the medium; and
6) the load is complete.

4.4.2 Unload states

Table 4 defines the states that may be reported in the VHF data descriptor (see 6.1.2.2) during unload operations. This information allows automation devices to coordinate loading and unloading of a medium with the DT device, and to obtain DT device activity status.

Table 4 — Unload states

Unload state	Bit in the VHF data descriptor					
	INXTN	RAA	MPRSNT	MSTD	MTHRD	MOUNTED
a) Medium mounted	0	0	1	1	1	1
b) DT device rewinding	1	0	1	1	1	0
c) Medium unthreaded, still unloading	1	0	1	1	0	0
d) Medium unseated, unloading or ejecting	1	0	1	0	0	0
e) DT device unloaded (hold point), seated	0	0	1	1	0	0
f) DT device unloaded (hold point), unseated	0	0	1	0	0	0
g) Medium ejected, presence detected	0	1	1	0	0	0
h) Medium ejected, presence not detected	0	1	0	0	0	0

Unload states (a) and (h) shall be supported by the ADC device server. States (b) through (g) (i.e., all other states) should be reported to accurately represent the states used by the DT device. Unload states may not be reported in the order listed in table 4.

To indicate an error in any of the listed states, or to report a state not listed, the RRQST bit in the VHF data descriptor shall be set to one and the INXTN bit shall be set to zero.

Unload state (a) represents the initial DT device state prior to receiving a request to unload.

Unload state (b) represents the initial DT device state after receiving a request to unload.

Unload state (c) represents the DT device state during the unload operation after the medium has been unthreaded.

Unload state (d) represents the DT device state during the unload operation after the medium has been unseated and the DT device state during the eject operation.

Unload state (e) represents the DT device state after unloading to the hold point, where the medium is still seated. An external stimulus (e.g., a request to eject or load) is needed to leave unload state (e).

Unload state (f) represents the DT device state after unloading to the hold point, where the medium is also unseated. An external stimulus (e.g., a request to eject or load) is needed to leave unload state (f).

Unload state (g) represents the DT device state after the medium is unloaded, ejected, and the DT device is still able to report medium present until the medium is completely removed.

Unload state (h) represents the DT device state after the medium is ejected and the presence of the medium is not detected (i.e., the DT device either does not support detection of medium presence at this state or the medium has been removed).

As an example, an unload to the hold point sequence may use states (a), (b), (c) and (e), or alternatively (a), (b), (c), (d), and (f). An unload to eject sequence may use states (a), (b), (c), (d), and (h).

4.5 Sense data masking

In the process of loading a medium into a DT device, it may be necessary to retry the load operation in order to overcome transient failures. Retrying the load operation may require removing and re-inserting the medium into the DT device. If an application client is testing the status of the RMC device server, then the application client may see an initial failure even though the loading eventually succeeds and the MOVE MEDIUM command to the SMC device returns GOOD status.

If the optional sense data masking feature is implemented, then the RMC device server's true status is not reported to the application client during automation device-initiated loads. Instead, the automation device may retry the load operation while the RMC device server reports that the load operation is still in progress to application clients.

If implemented, then the DT device shall enable sense data masking when the DT device begins loading a medium. The DT device shall disable sense data masking after any of the following occur:

a) loading succeeds;
b) loading fails and for a time equal to sense masking timeout value (SM_TOV) the automation device issues no medium access commands and does not remove and re-insert the medium;
c) the ADC device server receives a NOTIFY DATA TRANSFER DEVICE command with the LDFAIL bit set to one (see 5.2); or
d) the medium is removed and SM_TOV expires before the medium is re-inserted.

While sense data masking is enabled, then the RMC device server shall report status and sense data consistent with a normal loading operation.

During the SM_TOV period, if either the automation application client issues a medium access command or the automation device removes and re-inserts the medium, then the DT device shall not disable sense data masking. The SM_TOV timer shall be restarted when either the medium is re-inserted or the command is received.

After disabling sense data masking, the RMC device server shall report status and sense data indicating the load is in progress, and not report any failure that is encountered.

The value of SM_TOV is vendor-specific.

4.6 TapeAlert application client interface

The ADC device server supports a modified version of TapeAlert specified in SSC-2. As supported by the ADC device server, the TapeAlert flags represent states, and the state flags are not set to zero upon retrieval of the TapeAlert Response log page (see 6.1.3). Instead, the state flags are set to zero upon a change of the condition involved with the state (see table 5).

To facilitate accurate reporting of the conditions encountered by the DT device and allow the automation device to manage the information directly, the ADC device server does not maintain unique TapeAlert information for each I_T nexus, and the state flags are not affected by an I_T nexus loss condition (see SAM-3).

The application client is responsible for determining which flags have changed state upon subsequent retrieval of the TapeAlert Response log page, requiring the application client to maintain at least one previously retrieved TapeAlert Response log page in order to detect differences. The application client may maintain a state change history.

In conjunction with the VHF data descriptor (see 6.1.2.2), the TapeAlert state flags are a primary source of information about the DT device, and should be used to obtain DT device status information. Application clients may retrieve TapeAlert state flags at any time. Application clients should retrieve TapeAlert state flags after receiving from the DT device a VHF data descriptor with the TapeAlert Flags Changed (TAFC) bit to one.

The ADC device server shall maintain the TapeAlert state flags independently of the TapeAlert flags maintained by the RMC device server. Retrieving the state flags from the ADC device server shall not set the state flags maintained by the ADC device server to zero and shall not set the TapeAlert flags maintained by the RMC device server to zero. Retrieving TapeAlert flags from the RMC device server shall not set the state flags maintained by the ADC device server to zero.

The TapeAlert state flags shall be set to zero upon a logical unit reset to either the RMC or ADC device servers. The state flags shall be reported as new states following power on as conditions warrant. In addition to power on, other conditions and events that cause TapeAlert state flags to be set to zero are described in table 5.

Table 5 — Additional conditions that cause TapeAlert state flags to be set to zero (part 1 of 3)

Flag	Name	Additional clearing condition
01h	Read warning	Start of next medium load
02h	Write warning	Start of next medium load
03h	Hard error	Start of next medium load
04h	Media	Start of next medium load
05h	Read failure	Start of next medium load
06h	Write failure	Start of next medium load
07h	Media life	Start of next medium load
08h	Not data grade	Start of next medium load
09h	Write protect	Start of next medium load or removal of write protect
0Ah	No removal	After medium removal allowed
0Bh	Cleaning media	Start of next medium load
0Ch	Unsupported format	Start of next medium load or format change
0Dh	Recoverable mechanical cartridge failure	Start of next medium load
0Eh	Unrecoverable mechanical cartridge failure	After service resolution
0Fh	Memory chip in cartridge failure	Start of next medium load
10h	Forced eject	Start of next medium load

Table 5 — Additional conditions that cause TapeAlert state flags to be set to zero (part 2 of 3)

Flag	Name	Additional clearing condition
11h	Read only format	Start of next medium load or format change
12h	Tape directory corrupted on load	Start of next medium load
13h	Nearing media life	Start of next medium load
14h	Cleaning required	After successful cleaning or cause resolved
15h	Cleaning requested	After successful cleaning
16h	Expired cleaning media	Start of next medium load
17h	Invalid cleaning tape	Start of next medium load
18h	Retension requested	After successful retension
19h	Dual-port interface error	After interface returns to operation
1Ah	Cooling fan failure	After service resolution
1Bh	Power supply failure	After service resolution
1Ch	Power consumption	After power consumption returns to within specification
1Dh	Drive maintenance	After service resolution
1Eh	Hardware A	After service resolution
1Fh	Hardware B	After service resolution
20h	Interface	After interface returns to operation
21h	Eject media	Start of next medium load
22h	Microcode update fail	Start of next microcode update
23h	Drive humidity	After humidity returns to within specification
24h	Drive temperature	After temperature returns to within specification
25h	Drive voltage	After voltage returns to within specification
26h	Predictive failure	After service resolution
27h	Diagnostics required	After service resolution
28h- 2Eh	Obsolete	
2Fh- 31h	Reserved	
32h	Lost statistics	Start of next medium load
33h	Tape directory invalid at unload	Start of next medium load
34h	Tape system area write failure	Start of next medium load
35h	Tape system area read failure	Start of next medium load
36h	No start of data	Start of next medium load

Table 5 — Additional conditions that cause TapeAlert state flags to be set to zero (part 3 of 3)

Flag	Name	Additional clearing condition
37h	Loading failure	Start of next medium load
38h	Unrecoverable unload failure	After service resolution
39h	Automation interface failure	After service resolution
3Ah	Microcode failure	After service resolution
3Bh	WORM medium - Integrity Check Failed	Start of next medium load
3Ch	WORM medium - Overwrite Attempted	Start of next medium load
3Dh– 40h	Reserved	

Many of the state flags are set to zero at the start of the next medium load (see table 5), which is defined to be the DT device entering the next load state upon transition from load state (a) (see table 2). The next load state entered varies by DT device. If a load sequence is initiated from an unload hold point (i.e., unload state (e) or (f) in table 4), start of next medium load is defined to be the DT device entering the next load state upon transition from load states (c) or (e) (see table 4).

Other state flags are set to zero following service resolution (see table 5). Service resolution is beyond the scope of this standard.

4.7 Medium Auxiliary Memory attributes

ADC device servers shall not modify attributes of type Host. To change these attributes, the automation application client shall issue the WRITE ATTRIBUTE command (see SPC-3) to the RMC device server.

ADC device servers may modify the VOLUME IDENTIFIER attribute of type Device.

4.8 DT device primary ports

4.8.1 DT device primary port index

The DT device shall assign a primary port index value that uniquely identifies the DT device primary port relative to other DT device primary ports in the DT device, independent of DT device primary port type. Once assigned, the primary port index value for a DT device primary port shall not be changed as long as the DT device primary port remains on the DT device. A value of 00h is reserved. The primary port index value assigned to a DT device primary port may or may not be the same as the relative target port identifier (see SPC-3) assigned to the port.

4.8.2 Enabling and disabling DT device primary ports

A DT device shall allow the DT device primary port(s) to be disabled and enabled via MODE SELECT commands (see SPC-3) to the ADC device server that modify the DT Device Primary Port mode page (see 6.2.2.2).

The behavior of a DT device primary port if the port is disabled is protocol dependent (see 6.2.2.2).

The disabling of a DT device primary port shall be treated as an I_T nexus loss event (see SAM-3) for any existing I_T nexus associated with the disabled DT device primary port. If the command disabling a DT device primary port is received through the DT device primary port being disabled, then the ADC device server shall return status for the MODE SELECT command before disabling the DT device primary port.

4.9 Sequential mode operation

Some automation devices support a sequential mode of operation. When an automation device is configured in sequential mode, there is no SMC device server accessible in the SCSI domain. In sequential mode the automation device implicitly replaces a medium in the DT device with the next sequential medium in the automation device. A typical sequence of operations is:

1) the RMC device server receives and processes a command that requests that the medium be unloaded;
2) the automation device detects that an unload of the medium has occurred;
3) the automation device removes the current medium from the DT device and returns the medium to its storage element;
4) the automation device moves the next medium from a storage element to the DT device; and
5) the RMC device server becomes ready for access.

The automation device may use the HIU bit in the VHF data descriptor (see 6.1.2.2) to aid in the detection of an unloaded medium in step 2 of the sequence of operation shown in this subclause.

4.10 ADC tape data encryption control

4.10.1 ADC tape data encryption control introduction

If the DT device contains a logical unit that contains an RMC device server that reports itself as an SSC device in the standard INQUIRY data (see SPC-4), then the DT device may support tape data encryption and also may support ADC tape data encryption control. ADC tape data encryption control may support:

a) restricting the ability to establish or change a set of tape data encryption parameters;
b) establishing or changing tape data encryption parameters via the ADC device server; and
c) disabling tape data encryption algorithms.

If the DT device supports ADC tape data encryption control, then the ADC device server shall support the:

a) SECURITY PROTOCOL IN command specifying the Tape Data Encryption security protocol (see 6.3.2);
b) SECURITY PROTOCOL IN command specifying the Data Encryption Configuration security protocol (see 6.3.3);
c) SECURITY PROTOCOL OUT command (see SPC-4) specifying the Tape Data Encryption security protocol (see 6.3.4); and
d) SECURITY PROTOCOL OUT command specifying the Data Encryption Configuration security protocol (see 6.3.5).

An automation application client uses ADC tape data encryption control to control the tape data encryption capabilities of the DT device and the tape data encryption parameters of the DT device.

If the DT device supports ADC tape data encryption control, then the DT device accessed by the ADC device server shall contain a data encryption parameters control policy parameter. The value in the data encryption

parameters control policy parameter controls the ability to establish or change data encryption parameters within the physical device.

Table 6 shows the values of the data encryption parameters control policy.

Table 6 — Data encryption parameters control policy (part 1 of 2)

Policy Type	Policy Code	Description	Parameters Control		
			ADC Device Server	RMC Device Server	DT Device Management Interface
Vendor Specific	0000b	Vendor specific	VS	VS	VS
Open	0001b	No interface has taken exclusive control of data encryption parameters. This is the default setting for the data encryption parameters control policy.	A	A	A[c]
ADC exclusive	0010b	The ADC device server has exclusive control of the ability to establish or change data encryption parameters and shall report all data encryption algorithms in the list of algorithms reported by the DT device.	A	P[b]	P[d]
	0011b	The ADC device server has exclusive control of the ability to establish or change data encryption parameters and all algorithms are removed from the list of algorithms reported by the DT device (see SSC-3).	A	P[b]	P[d]

Parameters Control Key:

A = Allowed
If this device server or DT device management interface supports establishing or changing encryption parameters, then the DT device shall process a command from this device server or DT device management interface attempting to establish or change a set of data encryption parameters.

P = Prevented
The DT device shall reject a command from this device server or DT device management interface attempting to establish or change a set of data encryption parameters.

[a] The ADC device server shall terminate a SECURITY PROTOCOL OUT command that attempts to establish or change a set of data encryption parameters with CHECK CONDITION status with the sense key set to ILLEGAL REQUEST, and the additional sense code set to DATA ENCRYPTION CONFIGURATION PREVENTED.

[b] The RMC device server shall terminate a SECURITY PROTOCOL OUT command that attempts to establish or change a set of data encryption parameters. See the appropriate command set standard (e.g., SSC-3).

[c] The commands for establishing or changing a set of data encryption parameters via a DT device management interface are beyond the scope of this standard.

[d] The method for rejecting a command from a DT device management interface is beyond the scope of this standard.

Table 6 — Data encryption parameters control policy (part 2 of 2)

Policy Type	Policy Code	Description	Parameters Control		
			ADC Device Server	RMC Device Server	DT Device Management Interface
RMC exclusive	0100b	The RMC device server has exclusive control of the ability to establish or change data encryption parameters.	P[a]	A	P[d]
DT device management interface exclusive	0101b	The DT device management interface has exclusive control of the ability to establish or change data encryption parameters.	P[a]	P[b]	A[c]
	0110b – 1111b	Reserved			

Parameters Control Key:

A = Allowed
If this device server or DT device management interface supports establishing or changing encryption parameters, then the DT device shall process a command from this device server or DT device management interface attempting to establish or change a set of data encryption parameters.

P = Prevented
The DT device shall reject a command from this device server or DT device management interface attempting to establish or change a set of data encryption parameters.

[a] The ADC device server shall terminate a SECURITY PROTOCOL OUT command that attempts to establish or change a set of data encryption parameters with CHECK CONDITION status with the sense key set to ILLEGAL REQUEST, and the additional sense code set to DATA ENCRYPTION CONFIGURATION PREVENTED.

[b] The RMC device server shall terminate a SECURITY PROTOCOL OUT command that attempts to establish or change a set of data encryption parameters. See the appropriate command set standard (e.g., SSC-3).

[c] The commands for establishing or changing a set of data encryption parameters via a DT device management interface are beyond the scope of this standard.

[d] The method for rejecting a command from a DT device management interface is beyond the scope of this standard.

The data encryption parameters control policy type shall be set to Open following a:

a) hard reset condition; or
b) other vendor specific events.

An application client or DT device management interface should set the data encryption parameters control policy type to a value other than Open before sending a SECURITY PROTOCOL OUT command containing a page attempting to establish a set of data encryption parameters. An application client or DT device management interface may set the data encryption parameters control policy type to Open to return the data encryption parameters control policy to the default setting.

The data encryption parameters control policy type is set to Open by sending a SECURITY PROTOCOL OUT command specifying the Data Encryption Configuration security protocol with a Configure Encryption Policy page (see 6.3.5.3) to the ADC device server with the CONTROL POLICY CODE field set to 0001b.

The data encryption parameters control policy type is set to ADC exclusive by sending a SECURITY PROTOCOL OUT command specifying the Data Encryption Configuration security protocol with a Configure Encryption Policy page to the ADC device server with:

a) the CONTROL POLICY CODE field set to 0010b; or
b) the CONTROL POLICY CODE field set to 0011b.

The data encryption parameters control policy type is set to RMC exclusive by sending a SECURITY PROTOCOL OUT command specifying the Data Encryption Configuration security protocol with a Configure Encryption Policy page to the ADC device server with the CONTROL POLICY CODE field set to 0100b.

The data encryption control policy type is set to DT device management interface exclusive by:

a) sending a SECURITY PROTOCOL OUT command specifying the Data Encryption Configuration security protocol with a Configure Encryption Policy page to the ADC device server with the CONTROL POLICY CODE field set to 0101b; or
b) other vendor specific methods (e.g., a DT device management interface command beyond the scope of this standard).

4.10.2 Disabling a supported data encryption algorithm

The automation application client disables a data encryption algorithm (see SSC-3) by sending a SECURITY PROTOCOL OUT command specifying the Data Encryption Configuration security protocol with a Configure Data Encryption Algorithm Support page to the ADC device server with the ALGORITHM INDEX field in a data encryption algorithm support descriptor set to the algorithm index for the selected data encryption algorithm and the DISABLE bit set to one.

4.10.3 Reporting DT device data encryption algorithm support

A SECURITY PROTOCOL IN command specifying the Tape Data Encryption security protocol and the Data Encryption Capabilities page processed by the ADC device server returns the set of data encryption algorithms supported by the physical device (see SSC-3).

4.10.4 ADC tape data encryption control of data encryption parameters

4.10.4.1 ADC tape data encryption control of data encryption parameters introduction

The SECURITY PROTOCOL OUT command specifying the Data Encryption Configuration security protocol and the Configure Encryption Policy page (see 6.3.5.3) is used to configure a decryption parameters request policy, encryption parameters request policy, and encryption parameters request period (see SSC-3).

The SECURITY PROTOCOL OUT command specifying the Tape Data Encryption security protocol and a page that provides a set of data encryption parameters is used to establish or change a set of data encryption parameters for encryption, and establish or change a set of data encryption parameters for decryption (see SSC-3).

4.10.4.2 Reporting data encryption parameters requests

When configured to do so, the ADC device server shall notify the automation application client of data encryption parameters requests (e.g., the DT device includes an SSC-3 compliant device server and has a data encryption

parameters for encryption request indicator set to TRUE or has a data encryption parameters for decryption request indicator set to TRUE, see SSC-3) using the DT Device Status log page very high frequency data log parameter ESR bit (see 6.1.2.2), and the DT device ADC data encryption control status log parameter (see 6.1.2.4).

When processing an encryption parameters request, the ADC device server shall assign a data encryption parameters request sequence identifier to uniquely identify the encryption parameters request (see 6.1.2.4). The ADC device server shall maintain the data encryption parameters request sequence identifier until it processes a:

a) SECURITY PROTOCOL OUT command with a Data Encryption Parameters Complete page and a matching value in the PARAMETERS REQUEST SEQUENCE IDENTIFIER field; or
b) new encryption parameters request; or
c) hard reset condition.

If the DT device requires a set of data encryption parameters for data encryption, then the ADC device server shall:

1) set the encryption parameters request (EPR) bit in the DT device ADC data encryption control status log parameter to one; and
2) set the encryption service request (ESR) bit in the VHF data to one.

If the DT device requires a set of data encryption parameters for data decryption, then the ADC device server shall:

1) set the decryption parameters request (DPR) bit in the DT device ADC data encryption control status log parameter; and
2) set the ESR bit in the VHF data to one.

4.10.4.3 Providing a set of data encryption parameters

An automation application client may use ADC tape data encryption control to provide a set of data encryption parameters by:

1) monitoring the DT Device Status log page and the DT device ADC data encryption control status log parameter for the encryption parameters request (EPR) bit to be set to one, or the decryption parameters request (DPR) bit to be set to one;
2) sending a SECURITY PROTOCOL OUT command specifying the Tape Data Encryption security protocol and the Set Data Encryption page to the ADC device server to provide a set of tape data encryption parameters; and
3) sending a SECURITY PROTOCOL OUT command specifying the Tape Data Encryption security protocol and the Data Encryption Parameters Complete page to the ADC device server with the clear encryption parameters request (CEPR) bit set to one or the clear decryption parameters request bit (CDPR) set to one.

4.10.4.4 Data encryption parameters required values

The ADC device server shall terminate a SECURITY PROTOCOL OUT command (see SPC-4) attempting to establish or change a set of data encryption parameters with CHECK CONDITION status, with the sense key set to ILLEGAL COMMAND, and the additional sense code set to INVALID FIELD IN PARAMETER LIST if the data encryption parameters control policy type is set to ADC exclusive and:

a) the SCOPE field (see SSC-3) is set to a value other than 10b (i.e., ALL I_T NEXUS); or
b) the LOCK bit (see SSC-3) is set to one.

4.10.4.5 Key management errors

If the automation application client processes a DT device ADC data encryption control status log parameter (see 6.1.2.4) with the encryption parameters request (EPR) bit set to one and is unable to provide a set of data

encryption parameters for encryption, then the automation application client shall send a SECURITY PROTOCOL OUT command specifying the Tape Data Encryption security protocol and a Data Encryption Parameters Complete page (see 6.3.4.2) with the AUTOMATION COMPLETE RESULTS field set to the code indicating the reason that it was unable to provide a set of data encryption parameters for encryption.

If the automation application client processes a DT device ADC data encryption control status log parameter with the decryption parameters request (DPR) bit set to one and is unable to provide a set of data encryption parameters for decryption, then the automation application client shall send a SECURITY PROTOCOL OUT command specifying the Tape Data Encryption security protocol and a Data Encryption Parameters Complete page with the AUTOMATION COMPLETE RESULTS field set to the code indicating the reason that it was unable to provide a set of data encryption parameters for decryption.

If the automation application client receives a DT device ADC data encryption control status log parameter with the decryption parameters request (DPR) bit set to one and:

1) provides a set of data encryption parameters for decryption; and
2) the next DT device ADC data encryption control status log parameter contains a decryption parameters request for the same logical block (e.g., the value in the LOGICAL OBJECT NUMBER field in a Next Block Encryption Status page, see SSC-3).

then the automation application client shall:

a) send a SECURITY PROTOCOL OUT command specifying the Tape Data Encryption security protocol and a Data Encryption Parameters Complete page with the AUTOMATION COMPLETE RESULTS field set to 06h (see table 68); or
b) provide a set of data encryption parameters (e.g., a different set of data encryption parameters with the same key associated data, see SSC-3).

If the automation application client retries a failed set of data encryption parameters, then it shall have an encryption parameters retry limit. If the automation application client sends the DT device a set of data encryption parameters during process of a retry, then the automation application client shall keep track of the number of retries attempted and compare the number of retries to the retry limit before sending a new set of data encryption parameters. When the encryption parameters retry limit is reached the automation application client shall send a SECURITY PROTOCOL OUT command specifying the Tape Data Encryption security protocol and a Data Encryption Parameters Complete page with the AUTOMATION COMPLETE RESULTS field set to 06h (see table 68).

If the data encryption parameters period has expired in the DT device (e.g., the DT device includes an SSC-3 compliant device server and the data encryption period timer expired indicator is set to TRUE, see SSC-3), then the ADC device server shall:

1) set the ERROR TYPE field in the key management error data log parameter (see 6.1.2.5) to:
    a) 0001b (i.e., encryption parameters request error) if the encryption parameters request (EPR) bit in the DT device ADC data encryption control status log parameter (see 6.1.2.4) is set to one; or
    a) 0010b (i.e., decryption parameters request error) if the decryption parameters request (DPR) bit in the DT device ADC data encryption control status log parameter is set to one;
2) set the key timeout (KTO) bit in the key management error data log parameter (see 6.1.2.5) to one; and
3) set the key management error (KME) bit in the DT device ADC data encryption control status log parameter to one.

If the KME bit is set to one in the DT device ADC data encryption control status log parameter, then the automation application client should read the key management error data log parameter.

The PARAMETERS REQUEST ERROR SEQUENCE IDENTIFIER field of the key management error data log parameter indicates the data encryption parameters request sequence identifier of the request that has failed. If the param-

eters request sequence identifier does not match a known data encryption parameters request sequence identifier, then the key management error was for a previous data encryption parameters request and shall be ignored. If the data encryption parameters request sequence identifier is known, then the automation application client should abort processing the DT device ADC data encryption control status log parameter with the matching data encryption parameters request sequence identifier.

If the parameters request sequence specified by the PARAMETERS REQUEST ERROR SEQUENCE IDENTIFIER has failed, then the reason for the failure is:

a) a data encryption parameters request timeout if the KTO bit is set to one; or
b) the reason specified in the SENSE KEY field, ADDITIONAL SENSE CODE field, and the ADDITIONAL SENSE CODE QUALIFIER field if the KTO bit is set to zero.

If the abort (ABT) bit is set to one in the DT device ADC data encryption control status log parameters, then the automation application client should abort all data encryption parameters requests.

If the encryption parameters request (EPR) bit is set to one or the decryption parameters request (DPR) bit is set to one in the DT device ADC data encryption control status log parameter and a data encryption parameters request is in progress, then the automation application client should abort any data encryption parameters request with a data encryption parameters request sequence identifier that does not match the data encryption parameters request sequence identifier in the most recent DT device ADC data encryption control status log parameter.

5 Commands for automation/drive interface devices

5.1 Summary of commands for automation/drive interface devices

The command set for automation/drive interface devices is shown in table 7. Commands specified as mandatory in table 7 shall be implemented by automation/drive interface devices.

Table 7 — Command set for automation/drive interface (part 1 of 3)

Command name	Operation code	Type	Reference
ACCESS CONTROL IN	86h	O	SPC-3
ACCESS CONTROL OUT	87h	O	SPC-3
CHANGE ALIASES	A4h/0Bh [a]	O	SPC-3
EXTENDED COPY	83h	O	SPC-3
INQUIRY	12h	M	SPC-3
LOAD UNLOAD	1Bh	M	SSC-2
LOG SELECT	4Ch	O	SPC-3
LOG SENSE	4Dh	M	SPC-3
MODE SELECT(6)	15h	O	SPC-3
MODE SELECT(10)	55h	M	SPC-3
MODE SENSE(6)	1Ah	O	SPC-3
MODE SENSE(10)	5Ah	M	SPC-3
NOTIFY DATA TRANSFER DEVICE	9Fh/1Fh [a]	M	5.2
READ ATTRIBUTE	8Ch	M	SPC-3
READ BUFFER	3Ch	O	SPC-3
READ MEDIA SERIAL NUMBER	ABh/01h [a]	O	SPC-3

Type Key: M = mandatory
O = optional

[a] This command is defined by a combination of operation code and service action. The operation code value is shown preceding the slash and the service action value is shown after the slash.

[b] This command is subject to the readiness of the removable medium (i.e., the logical unit is able to process medium-access commands without returning CHECK CONDITION status). Other commands may be subject to readiness of the removable medium due to vendor-specific features.

[c] This command is subject to the readiness of the removable medium when the MEDIA bit is set to one.

[d] Only mandatory for devices that include an SSC-3 compliant device server.

[e] Only self test shall be mandatory.

Table 7 — Command set for automation/drive interface (part 2 of 3)

Command name	Operation code	Type	Reference
RECEIVE COPY RESULTS	84h	O	SPC-3
RECEIVE DIAGNOSTIC RESULTS	1Ch	O	SPC-3
REPORT ALIASES	A3h/0Bh [a]	O	SPC-3
REPORT DENSITY SUPPORT [c]	44h	M [d]	SSC-3
REPORT DEVICE IDENTIFIER	A3h/05h [a]	O	SPC-3
REPORT LUNS	A0h	M	SPC-3
REPORT PRIORITY	A3h/0Eh [a]	O	SPC-3
REPORT SUPPORTED OPERATION CODES	A3h/0Ch [a]	M	SPC-3
REPORT SUPPORTED TASK MANAGEMENT FUNCTIONS	A3h/0Dh [a]	O	SPC-3
REPORT TARGET PORT GROUPS	A3h/0Ah [a]	O	SPC-3
REPORT TIMESTAMP	A3h/0Fh [a]	O	SPC-3
REQUEST SENSE	03h	M	SPC-3
SECURITY PROTOCOL IN	A2h	O	SPC-4
SECURITY PROTOCOL OUT	B5h	O	SPC-4
SEND DIAGNOSTIC	1Dh	M [e]	SPC-3
SET DEVICE IDENTIFIER	A4h/06h [a]	O	SPC-3
SET MEDIUM ATTRIBUTE	A9h/1Fh [a]	O	5.3
SET PRIORITY	A4h/0Eh [a]	O	SPC-3
SET TARGET PORT GROUPS	A4h/0Ah [a]	O	SPC-3

Type Key: M = mandatory
O = optional

[a] This command is defined by a combination of operation code and service action. The operation code value is shown preceding the slash and the service action value is shown after the slash.

[b] This command is subject to the readiness of the removable medium (i.e., the logical unit is able to process medium-access commands without returning CHECK CONDITION status). Other commands may be subject to readiness of the removable medium due to vendor-specific features.

[c] This command is subject to the readiness of the removable medium when the MEDIA bit is set to one.

[d] Only mandatory for devices that include an SSC-3 compliant device server.

[e] Only self test shall be mandatory.

Table 7 — Command set for automation/drive interface (part 3 of 3)

Command name	Operation code	Type	Reference
SET TIMESTAMP	A4h/0Fh [a]	O	SPC-3
TEST UNIT READY [b]	00h	M	SPC-3
WRITE ATTRIBUTE	8Dh	O	SPC-3
WRITE BUFFER	3Bh	O	SPC-3

Type Key: M = mandatory
O = optional

[a] This command is defined by a combination of operation code and service action. The operation code value is shown preceding the slash and the service action value is shown after the slash.

[b] This command is subject to the readiness of the removable medium (i.e., the logical unit is able to process medium-access commands without returning CHECK CONDITION status). Other commands may be subject to readiness of the removable medium due to vendor-specific features.

[c] This command is subject to the readiness of the removable medium when the MEDIA bit is set to one.

[d] Only mandatory for devices that include an SSC-3 compliant device server.

[e] Only self test shall be mandatory.

5.2 NOTIFY DATA TRANSFER DEVICE command

The NOTIFY DATA TRANSFER DEVICE command (see table 8) notifies the ADC device server of specific events. The NOTIFY DATA TRANSFER DEVICE command does not represent the complete current state of the automation device and is not intended to be sent upon every change in the automation device's state.

If a NOTIFY DATA TRANSFER DEVICE command is received from an I_T nexus with a pending unit attention condition (i.e., before the ADC device server reports CHECK CONDITION status), then the ADC device server shall process the NOTIFY DATA TRANSFER DEVICE command and shall not clear the unit attention condition.

The automation application client shall send the NOTIFY DATA TRANSFER DEVICE command when any of the events that the NOTIFY DATA TRANSFER DEVICE command reports have occurred. Multiple events may be reported in the same NOTIFY DATA TRANSFER DEVICE command. The command shall report only those events that have not been previously reported.

Table 8 — NOTIFY DATA TRANSFER DEVICE command

Bit / Byte	7	6	5	4	3	2	1	0
0	OPERATION CODE (9Fh)							
1	Reserved			SERVICE ACTION (1Fh)				
2	Reserved							LDFAIL
3	Reserved			SOCC	BUA	NRSC	IDC	MDC
4	ASC							
5	ASCQ							
6	Reserved							
14								
15	CONTROL							

A load failed (LDFAIL) bit set to one specifies the automation device has detected that the RRQST bit in the VHF data descriptor (see 6.1.2.2) is set to one while the DT device is attempting to load a medium, and the automation device has completed all recovery attempts. A LDFAIL bit set to zero specifies that a load failure has not been detected.

The MDC bit, IDC bit, NRSC bit, and SOCC bit are used to specify that cached SMC data may require refreshing (see 4.3.5).

A supported operation codes changed (socc) bit set to one specifies that the list of operation codes supported by the remote SMC device server has changed. Upon successful completion of a NOTIFY DATA TRANSFER command with the socc bit set to one, the use of any cached operation code list shall be discontinued until the cached list has been refreshed. A socc bit set to zero specifies that the list of operation codes supported by the remote SMC device server has not changed. If the CACHE bit in the SMC Logical Unit descriptor is set to one, then the ADC device server shall support the SOCC bit set to one, but shall ignore the bit if the operation codes supported by the remote SMC device server are not cached.

A broadcast unit attention (BUA) bit set to one specifies that the ASC field and ASCQ field contain the additional sense data that shall be used by the local SMC device server to establish a unit attention condition for all I_T nexuses accessible via the DT device primary ports. If none of the known I_T nexuses are able to have a unit attention condition established by the device server due to insufficient resources, then the device server shall terminate the NOTIFY DATA TRANSFER DEVICE command with a CHECK CONDITION status and set the sense

key to ILLEGAL REQUEST and the additional sense code to INSUFFICIENT RESOURCES. If the additional sense data in the ASC field and ASCQ field is set to NOT READY TO READY CHANGE, MEDIUM MAY HAVE CHANGED, then the remote SMC device server ready state has transitioned to accessible (see 4.3.5). A BUA bit set to zero specifies that the ASC field and ASCQ field contents shall not be used by the local SMC device server to establish a unit attention condition for any I_T nexuses accessible via the DT device primary ports.

NOTE 2 The return of GOOD status for a NOTIFY DATA TRANSFER DEVICE command with the BUA bit set to one does not guarantee delivery of the unit attention condition to every I_T nexus known to the DT device.

A not ready state changed (NRSC) bit set to one indicates that the remote SMC device server ready state has transitioned to indicate not accessible (see 4.3.5). A NRSC bit set to one may also indicate that the remote SMC device server ready state already indicated not accessible state and the sense data changed. When the NRSC bit is set to one, the ASC field and ASCQ field contain additional sense data appropriate to the condition. Upon successful completion of a NOTIFY DATA TRANSFER command with the NRSC bit set to one, the cached ready state and additional sense data shall be updated. A NRSC bit set to zero indicates that the remote SMC device server ready state has not transitioned to indicate not accessible state, nor has the additional sense data changed if the remote SMC device server ready state already indicated not accessible. If the CACHE bit in the SMC Logical Unit descriptor is set to one, then the ADC device server shall support the NRSC bit set to one, but shall ignore the NRSC bit if the ready state is not cached.

If the NRSC bit and the BUA bit are both set to one, or if both bits are set to zero and either the ASC field or the ASCQ field is not set to zero, then the command shall be terminated with a CHECK CONDITION status. The sense key shall be set to ILLEGAL REQUEST and the additional sense code shall be set to INVALID FIELD IN CDB.

An INQUIRY data changed (IDC) bit set to one specifies that the contents of the standard INQUIRY data or any VPD page data reported by the remote SMC device server have changed. Upon successful completion of a NOTIFY DATA TRANSFER command with the IDC bit set to one, the use of any cached INQUIRY data or VPD pages shall be discontinued until the cached data have been refreshed. An IDC bit set to zero specifies that the contents have not changed. If the CACHE bit in the SMC Logical Unit descriptor is set to one, then the ADC device server shall support the IDC bit set to one, but shall ignore the bit if INQUIRY data is not cached.

A mode data changed (MDC) bit set to one specifies that the contents of a mode page or mode parameter header reported by the remote SMC device server have changed. Upon successful completion of a NOTIFY DATA TRANSFER command with the MDC bit set to one, the use of any cached mode data by the local SMC device server (see 4.3.2) shall be discontinued until the cached mode data has been refreshed. A MDC bit set to zero specifies that the contents have not changed. If the CACHE bit in the SMC Logical Unit descriptor is set to one (see 6.2.2.3.3), then the ADC device server shall support the MDC bit set to one, but shall ignore the bit if mode data is not cached.

5.3 SET MEDIUM ATTRIBUTE command

5.3.1 SET MEDIUM ATTRIBUTE command introduction

The SET MEDIUM ATTRIBUTE command (see table 9) is used to pass attributes of the medium to the ADC device server. The device server may use any attributes set by this command to:

a) add the attribute to log entries the DT device creates;
b) add the attribute to the device type specific area in the MAM (see SPC-3);
c) report the attribute to application clients in response to commands or other means beyond the scope of this standard; or
d) other uses beyond the scope of this standard.

Table 9 — SET MEDIUM ATTRIBUTE command

Bit / Byte	7	6	5	4	3	2	1	0
0	OPERATION CODE (A9h)							
1	Reserved			SERVICE ACTION (1Fh)				
2	Reserved							
5								
6	(MSB)							
9	PARAMETER LIST LENGTH							(LSB)
10	Reserved							
11	CONTROL							

See SPC-3 for the description of the PARAMETER LIST LENGTH field.

The device server shall retain the attributes sent with a SET MEDIUM ATTRIBUTE command when no medium is present in the device until:

a) a SET MEDIUM ATTRIBUTE command is processed that changes the attribute; or
b) a logical unit reset condition occurs.

Attributes established when no medium is present shall be applied to the next medium loaded.

All medium attributes set by the SET MEDIUM ATTRIBUTE command shall be cleared by the device server when the medium is removed from the device.

5.3.2 SET MEDIUM ATTRIBUTE parameter list format

The parameter list shall have the format shown in table 10. Medium attributes should be listed in ascending numerical order based on the ATTRIBUTE IDENTIFIER field (see 5.3.3).

Table 10 — SET MEDIUM ATTRIBUTE parameter list format

Bit / Byte	7	6	5	4	3	2	1	0
0	(MSB)							
3	PARAMETER DATA LENGTH (n-3)							(LSB)
	Medium attribute list							
4	Medium attribute (first) (see 5.3.3)							
	. .							
n	Medium attribute (last) (see 5.3.3)							

The PARAMETER DATA LENGTH field should contain the number of bytes of attribute data.

The format of the medium attributes is described in 5.3.3.

No medium attributes shall be changed and the SET MEDIUM ATTRIBUTE command shall be terminated with CHECK CONDITION status with the sense key set to ILLEGAL REQUEST and the additional sense code set to INVALID FIELD IN PARAMETER LIST, if the parameter data contains any of the following:

a) a medium attribute with an attribute length that exceeds the value shown in table 12;
b) a medium attribute with an unsupported or reserved FORMAT field (see 5.3.3) value;
c) a medium attribute with unsupported ATTRIBUTE VALUE field (see 5.3.3) contents and a non-zero ATTRIBUTE LENGTH field value; or
d) a medium attribute with a value in the FORMAT field that does not match the value shown table 12.

If the SET MEDIUM ATTRIBUTE command parameter data contains a medium attribute with an ATTRIBUTE LENGTH field set to zero, then one of the following actions shall occur:

a) If the medium attribute is supported, the medium attribute's value shall be cleared; or
b) If the medium attribute is not supported, the medium attribute shall be ignored and this shall not be considered an error.

5.3.3 SET MEDIUM ATTRIBUTE attribute format

Each medium attribute shall be communicated between the application client and device server in the format shown in table 11.

Table 11 — SET MEDIUM ATTRIBUTE attribute format

Bit / Byte	7	6	5	4	3	2	1	0
0	(MSB)							
1	ATTRIBUTE IDENTIFIER							(LSB)
2	Reserved						FORMAT	
3	Reserved							
4	(MSB)							
5	ATTRIBUTE LENGTH (n-5)							(LSB)
6								
n	ATTRIBUTE VALUE							

The ATTRIBUTE IDENTIFIER field (see table 12) specifies the medium attribute to be set.

Table 12 — ATTRIBUTE IDENTIFIER **field**

Code	Description	Format	Maximum length (bytes)
0000h	Volume identifier (see SMC-3)	ASCII	32
0001h-FF7Fh	Reserved		
FF80h-FFFFh	Vendor specific		

The FORMAT field (see table 13) specifies the format of the data in the ATTRIBUTE VALUE field.

Table 13 — FORMAT **field**

Code	Name	Description
00b	BINARY	The ATTRIBUTE VALUE field contains binary data.
01b	ASCII	The ATTRIBUTE VALUE field contains left-aligned ASCII data.
10b-11b		Reserved

The ATTRIBUTE LENGTH field specifies the length in bytes of the ATTRIBUTE VALUE field.

The ATTRIBUTE VALUE field contains the intended value of the medium attribute.

6 Parameters for automation/drive interface devices

6.1 Log parameters

6.1.1 Log parameters overview

This subclause defines the log pages and log parameters for ADC device servers.

The log page codes for ADC device servers are defined in table 14.

Table 14 — Log page codes (part 1 of 2)

Page code	Description	Support requirement	Reference
00h	Supported Log Pages page	Mandatory	SPC-3
01h	Buffer Overrun/Underrun log page	Optional	SPC-3
02h	Write Error Counter log page	Optional	SPC-3
03h	Read Error Counter log page	Optional	SPC-3
04h	Read Reverse Error Counter log page	Optional	SPC-3
05h	Verify Error Counter log page	Optional	SPC-3
06h	Non-Medium Error log page	Optional	SPC-3
07h	Last *n* Error Events log page	Optional	SPC-3
08h	Format Status log page	Optional	SPC-3
09h - 0Ah	Reserved		
0Bh	Last *n* Deferred Error Events log page	Optional	SPC-3
0Ch	Sequential-Access Device log page	Optional	SSC-2
0Dh	Temperature log page	Optional	SPC-3
0Eh	Start-Stop Cycle Counter log page	Optional	SPC-3
0Fh	Application Client log page	Optional	SPC-3
10h	Self-Test Results log page	Optional	SPC-3
11h	DT Device Status log page	Mandatory	6.1.2
12h	TapeAlert Response log page	Mandatory	6.1.3
13h	Requested Recovery log page	Mandatory	6.1.4
14h	Device Statistics log page	Optional	SSC-3
15h	Service Buffers Information log page	Optional	6.1.5
16h	Tape Diagnostic Data log page	Optional [a]	SSC-3

[a] Mandatory if the TDDEC bit in the VHF data descriptor is supported.

Table 14 — Log page codes (part 2 of 2)

Page code	Description	Support requirement	Reference
17h	Reserved		
18h	Protocol Specific Port log page	Optional	SPC-3
19h - 2Eh	Reserved		
2Fh	Informational Exceptions log page	Optional	SPC-3
30h - 3Eh	Vendor-specific log pages		
3Fh	Reserved		

[a] Mandatory if the TDDEC bit in the VHF data descriptor is supported.

Changes to log parameters caused by either LOG SELECT commands or other DT device operation of an RMC device server shall not be reflected by changes in the corresponding parameters reported by the ADC device server (i.e., log parameters of ADC and RMC device servers in the same DT device are independent). Changes in log parameters caused by either LOG SELECT commands or other DT device operation of an ADC device server shall not be reflected by changes in the corresponding parameters reported by the RMC device server.

6.1.2 DT Device Status log page

6.1.2.1 DT Device Status log page overview

The DT Device Status log page (see table 15) defines log information pertaining to the DT device and DT device primary ports.

Table 15 — DT Device Status log page

Bit / Byte	7	6	5	4	3	2	1	0
0	Reserved		PAGE CODE (11h)					
1	Reserved							
2	(MSB)		PAGE LENGTH (n-3)					
3								(LSB)
4	DT Device Status log parameters							
n								

See SPC-3 for a description of the PAGE CODE and PAGE LENGTH fields.

Table 16 defines the DT Device Status log page parameter codes.

Table 16 — DT Device Status log page parameter codes

Parameter code	Description	Reference
0000h	Very high frequency data	6.1.2.2
0001h	Very high frequency polling delay	6.1.2.3
0002h - 00FFh	DT device ADC data encryption control status	6.1.2.4
0003h	Key management error data	6.1.2.5
004h-00FFh	Reserved	
100h	Obsolete	
0101h - 01FFh	DT device primary port status	6.1.2.6
0200h - 7FFFh	Reserved	
8000h - FFFFh	Vendor-specific	

6.1.2.2 Very high frequency data log parameter

The very high frequency data log parameter format is shown in table 17.

Table 17 — Very high frequency data log parameter format

Bit / Byte	7	6	5	4	3	2	1	0
0	(MSB)							
1	PARAMETER CODE (0000h)							(LSB)
2	DU (0)	DS (1)	TSD (0)	ETC (0)	TMC (00)		LBIN (1)	LP (1)
3	PARAMETER LENGTH (04h)							
4	VHF data descriptor							
7								

The PARAMETER CODE field shall be set to 0000h to indicate the very high frequency data log parameter.

See SPC-3 for descriptions of the DU bit, DS bit, TSD bit, ETC bit, TMC field, LBIN bit, and LP bit. These bits and fields shall be set to the values shown in table 17.

The PARAMETER LENGTH field shall be set to 04h.

The VHF data descriptor is defined in table 18.

Table 18 — VHF data descriptor

Bit Byte	7	6	5	4	3	2	1	0
0	PAMR	HIU	MACC	CMPR	WRTP	CRQST	CRQRD	DINIT
1	INXTN	Rsvd	RAA	MPRSNT	Rsvd	MSTD	MTHRD	MOUNTED
2	DT DEVICE ACTIVITY							
3	VS	Reserved	TDDEC	EPP	ESR	RRQST	INTFC	TAFC

The prevent/allow medium removal (PAMR) bit shall be set to one when removal of the medium in the DT device is prevented as the result of the RMC device server processing a PREVENT ALLOW MEDIUM REMOVAL command (see SPC-3 or the relevant command standard). The PAMR bit shall be set to zero when removal of the medium in the DT device is allowed as defined by the PREVENT ALLOW MEDIUM REMOVAL command.

The host initiated unload (HIU) bit shall be set to one when the DT device reaches any one of the unload states (e) - (h) (see table 4) due to the RMC device server receiving a LOAD UNLOAD command (see SSC-2) with the LOAD bit set to zero. The HIU bit shall be set to zero when the DT device transitions to any state in table 2 or table 4 other than unload states (e) - (h) in table 4. The HIU bit may be set to zero following a logical unit reset of the RMC or ADC device servers.

NOTE 3 The HIU bit may facilitate sequential mode operation (see 4.9).

A medium auxiliary memory accessible (MACC) bit set to one indicates that the medium is located at a position where the MAM is accessible. A MACC bit set to zero indicates that the MAM is not accessible. If the MACC bit is set to one, then the ADC device server shall also support commands to access the MAM. If the MACC bit is supported, then the MACC bit should only be set to one if the MPRSNT bit is set to one. The MACC bit is only applicable for DT devices and media that support MAM.

A compress (CMPR) bit set to one indicates that the DT device currently has data compression enabled. A CMPR bit set to zero indicates that compression is not enabled.

A write protect (WRTP) bit set to one indicates that any current medium is physically write protected. A WRTP bit set to zero indicates that any current medium is not physically write protected. The WRTP bit is only valid if the MPRSNT bit is set to one. The WRTP bit should be set to zero if the MPRSNT bit is set to zero.

NOTE 4 Physically write protected refers to any mechanism used within the medium shell itself to write protect the medium (e.g., sliding windows or tabs) and not logical states of write protection caused by commands to the DT device.

A cleaning requested (CRQST) bit set to one indicates that the DT device has requested a head cleaning. A CRQST bit set to zero indicates that no cleaning is requested.

A cleaning required (CRQRD) bit set to one indicates that a head cleaning operation is required before a data medium is able to reach load state (i) (see 4.4.1), and that normal operation may not be possible if the head cleaning operation is not performed. A CRQRD bit set to zero indicates that urgent cleaning is not required. It shall not be considered an error for the CRQRD bit and the CRQST bit to both be set to one.

A DT device initialized (DINIT) bit set to one indicates that the DT device is able to return valid very high frequency data. A DINIT bit set to zero indicates DT device initialization is required or incomplete and the values of other bits in the very high frequency data log parameter are indeterminate.

NOTE 5 In addition to reliance on indication of initialization completion, reliance on returned values should also take into consideration conditions indicated by changes in Tape Alert flag status, and process those first as needed.

The in transition (INXTN) bit governs all of the other bits in byte 1 to indicate the stability of the values returned and whether state transitions are taking place. An INXTN bit set to one indicates that the state currently reflected by all of the other bits in byte 1 is in transition, because the DT device is transitioning to another state. An INXTN bit set to zero indicates that the DT device is in the state reflected by all of the other bits in byte 1 and is making no attempt to leave this state. When the recovery requested (RRQST) bit is set to one, the INXTN bit shall be set to zero.

A robotic access allowed (RAA) bit set to one indicates that the automation device may move a medium to or from the DT device. A RAA bit set to zero indicates that the automation device should not move a medium to or from the DT device. The DT device should indicate that access is allowed by the robotics if a medium may be successfully inserted into or removed from the DT device.

NOTE 6 The RAA bit is not intended to reflect the value of any PREVENT ALLOW MEDIUM REMOVAL command settings (see SPC-3), nor the ability of the automation device to issue commands to the DT device.

A medium present (MPRSNT) bit set to one indicates that the DT device detects the presence of a medium. A MPRSNT bit set to zero indicates that the DT device does not detect a medium present.

A medium seated (MSTD) bit set to one indicates that the medium is mechanically seated within the loading mechanism (i.e., the physical loading process has completed). A MSTD bit set to zero indicates that the medium is not seated, and that further mechanical motion remains in order to complete the loading process, exclusive of tape threading.

A medium threaded (MTHRD) bit set to one indicates that the medium has been threaded by the DT device, such that tape motion operations are possible. A MTHRD bit set to zero indicates that the medium has not been threaded.

NOTE 7 The value of the MTHRD bit may or may not correspond to the DT device responding with GOOD status to a TEST UNIT READY command (see SPC-3), as additional processing may be required by the DT device after threading before the logical unit becomes ready.

A MOUNTED bit set to one indicates that the DT device is in load state (i) (see 4.4.1). The MOUNTED bit set to one may correspond to the RMC device server being able to respond to a TEST UNIT READY command with GOOD status, however when a cleaning or microcode image medium is loaded the RMC device server may respond to a TEST UNIT READY command with a CHECK CONDITON status with the sense key set to NOT READY. A MOUNTED bit set to zero indicates that the DT device is not in load state (i).

The DT DEVICE ACTIVITY field is used to describe the current activity of the DT device (see table 19).

Table 19 — DT DEVICE ACTIVITY **field**

Code	Description
00h	No DT device activity
01h	Cleaning operation in progress
02h	Medium is being loaded
03h	Medium is being unloaded
04h	Other medium activity
05h	Reading from medium
06h	Writing to medium
07h	Locating medium
08h	Rewinding medium
09h	Erasing medium
0Ah	Formatting medium
0Bh	Calibrating medium
0Ch	Other DT device activity
0Dh	Microcode update in progress
0Eh	Reading encrypted from medium
0Fh	Writing encrypted to medium
10h-7Fh	Reserved
80h-FFh	Vendor-specific DT device activity

A tape diagnostic data entry created (TDDEC) bit set to one indicates that the DT device has created a new Tape Diagnostic Data log page entry (see SSC-3) since the last retrieval of any of the parameters from the Tape Diagnostic Data log page by this I_T nexus. A TDDEC bit set to zero indicates that the DT device has not created a new Tape Diagnostic Data log page entry since the last retrieval of any of the parameters from the Tape Diagnostic Data log page by this I_T nexus.

An encryption parameters present (EPP) bit set to one indicates that the DT device has a set of saved data encryption parameters with either the ENCRYPTION MODE field set to a value other than DISABLE (see SSC-3) or the DECRYPTION MODE field set to a value other than DISABLE (see SSC-3) associated with any I_T nexus or a DT device management interface. An EPP bit set to zero indicates that the DT device does not have a set of saved data encryption parameters with either the ENCRYPTION MODE field set to a value other than DISABLE or the DECRYPTION MODE field set to a value other than DISABLE associated with any I_T nexus or a DT device management interface.

An encryption service request (ESR) bit set to one indicates that:

a) at least one bit in the SERVICE REQUEST INDICATORS field in the DT device ADC data encryption control status log parameter has been set to one since the last retrieval of the DT device ADC data encryption control status log parameter (see 6.1.2.4) by this I_T nexus; and
b) at least one bit in the SERVICE REQUEST INDICATORS field in the DT device ADC data encryption control status log parameter is set to one.

The ADC device server sets the ESR bit to zero after retrieval of the DT device ADC data encryption control status log parameter by this I_T nexus. An ESR bit set to zero indicates:

a) that no bits in the SERVICE REQUEST INDICATORS field in the DT device ADC data encryption control status log parameters have been set to one since the last retrieval of the DT device ADC data encryption control status log parameter by this I_T nexus; or
b) that all of the bits in the SERVICE REQUEST INDICATORS field in the DT device ADC data encryption control status log parameter are set to zero.

The recovery requested (RRQST) bit shall be set to one to indicate that the DT device has detected an error and that one or more requested recovery procedures are available via the Requested Recovery log page (see 6.1.4). A RRQST bit set to zero indicates that no recovery procedure is requested. The RRQST bit shall remain set to one as long as a recovery procedure is available. When the RRQST bit is set to one, the INXTN bit shall be set to zero.

NOTE 8 The Requested Recovery log page may indicate that a recovery procedure is not requested or not defined.

An interface changed (INTFC) bit set to one indicates that one or more fields in the DT device primary port status log parameters (see 6.1.2.6) have changed since the last retrieval of any of the DT device primary port status log parameters from the DT Device Status log page by this I_T nexus. If one or more fields in the DT device primary port status log parameters have changed since a primary port has been enabled, then the device server may set the INTFC bit to one before any of the DT device primary port status log parameters have been retrieved from the DT Device Status log page by this I_T nexus. An INTFC bit set to zero indicates that no fields in the DT device primary port status log parameters have changed since the last retrieval of any of the DT device primary port status log parameters by this I_T nexus. An INTFC bit set to zero may indicate that none of the DT device primary port status log parameters from the DT Device Status log page have been retrieved by this I_T nexus since the last hard reset condition.

A TapeAlert state flag changed (TAFC) bit set to one indicates that at least one TapeAlert state flag has changed from its previous value since the last retrieval of the TapeAlert Response log page (see 6.1.3) by this I_T nexus. The ADC device server sets the TAFC bit to zero after retrieval of the TapeAlert Response log page by this I_T nexus. A TAFC bit set to zero indicates that no TapeAlert state flag has changed. There may not be any difference in the TapeAlert state flags upon retrieval if the state changed again between the time of reporting through the TAFC bit and retrieving the TapeAlert Response log page. This should not be considered an error. Pending TapeAlert state flags may affect the reliability of the values returned in other bits within the VHF data descriptor (see 6.1.2.2).

6.1.2.3 Very high frequency polling delay log parameter

The very high frequency polling delay log parameter format is shown in table 20.

The PARAMETER CODE field shall be set to 0001h to indicate the very high frequency polling delay log parameter.

See SPC-3 for descriptions of the DU bit, DS bit, TSD bit, ETC bit, TMC field, LBIN bit, and LP bit. These bits and fields shall be set to the values shown in table 20.

The PARAMETER LENGTH field shall be set to 02h to allow transfer of the complete parameter.

Table 20 — Very high frequency polling delay log parameter format

Bit / Byte	7	6	5	4	3	2	1	0
0	(MSB)	PARAMETER CODE (0001h)						
1								(LSB)
2	DU (0)	DS (1)	TSD (0)	ETC (0)	TMC (00)		LBIN (1)	LP (1)
3	PARAMETER LENGTH (02h)							
4	(MSB)	VHF POLLING DELAY						
5								(LSB)

The VHF POLLING DELAY field indicates the minimum delay in milliseconds the automation application client should wait before requesting the DT Device Status log page again.

6.1.2.4 DT device ADC data encryption control status log parameter

The DT device ADC data encryption status log parameter format is shown in table 21.

Table 21 — DT device ADC data encryption control status log parameter format

Bit / Byte	7	6	5	4	3	2	1	0
0	(MSB)	PARAMETER CODE (0002h)						
1								(LSB)
2	DU (0)	DS (1)	TSD (0)	ETC (0)	TMC (00)		LBIN (1)	LP (1)
3	PARAMETER LENGTH (08h)							
4	SERVICE REQUEST INDICATORS							
5								
6	(MSB)	PARAMETERS REQUEST SEQUENCE IDENTIFIER						
9								(LSB)
10	Reserved							
11								

The PARAMETER CODE field shall be set to 0002h to indicate the DT device ADC data encryption control status log parameter.

See SPC-3 for descriptions of the DU bit, DS bit, TSD bit, ETC bit, TMC field, LBIN bit, and LP bit. These bits and fields shall be set to the values shown in table 21.

The PARAMETER LENGTH field shall be set to 08h.

The SERVICE REQUEST INDICATORS field is shown in table 22.

Table 22 — SERVICE REQUEST INDICATORS field

Bit / Byte	7	6	5	4	3	2	1	0
0	Reserved							
1	EPR	DPR	KME	ABT	Reserved			

An encryption parameters request (EPR) bit set to one indicates that the ADC device server requests a set of data encryption parameters for encryption from the automation application client. The ADC device server shall set the EPR bit to one when the DT device indicates a set of data encryption parameters for encryption is required (e.g., the DT device includes an SSC-3 compliant device server and has the data encryption parameters for encryption request indicator set to TRUE, see SSC-3). If the EPR bit is set to one, then the automation application client should abort any data encryption parameters request in progress with a data encryption parameters request identifier that is different from the value specified in the PARAMETERS REQUEST SEQUENCE IDENTIFIER field. If the EPR bit is set to one, then the abort (ABT) bit shall be set to zero.

An EPR bit set to zero indicates that the ADC device server does not request a set of data encryption parameters for encryption from the automation application client. The ADC device server shall set the EPR bit to zero and shall set the data encryption parameters for encryption request indicator in the DT device to FALSE when:

a) it successfully processes a SECURITY PROTOCOL OUT command, with the SECURITY PROTOCOCOL field set to Tape Data Encryption and with the clear encryption parameters request (CEPR) bit in a Data Encryption Parameters Complete page set to one;
b) it successfully processes a SECURITY PROTOCOL OUT command, with the SECURITY PROTOCOCOL field set to Tape Data Encryption and with the AUTOMATION COMPLETE RESULTS field in a Data Encryption Parameters Complete page set to a nonzero value; or
c) the data encryption parameters for encryption indicator in the DT device is set to FALSE (e.g., the DT Device includes an SSC-3 compliant device server and has set the data encryption parameters for encryption indicator to FALSE after a data encryption parameters timer has expired).

A decryption parameters request (DPR) bit set to one indicates that the ADC device server requests a set of encryption parameters for decryption from the automation application client. The ADC device server shall set the DPR bit to one when the DT device indicates a set of data encryption parameters for decryption is required (e.g., the DT device includes an SSC-3 compliant device server and has the data encryption parameters for encryption request indicator set to TRUE, see SSC-3). If the DPR bit is set to one, then the automation application client should abort any data encryption parameters request in progress with a data encryption parameters request sequence identifier that is different from the value specified in the PARAMETERS REQUEST SEQUENCE IDENTIFIER field. If the DPR bit is set to one, then the ABT bit shall be set to zero.

A DPR bit set to zero indicates that the ADC device server does not request a set of data encryption parameters for decryption from the automation application client. The ADC device server shall set the DPR bit to zero and shall set the data encryption parameters for decryption request indictor in the DT device to FALSE if:

a) it successfully processes a SECURITY PROTOCOL OUT command, with the SECURITY PROTOCOCOL field set to Tape Data Encryption and with the clear decryption parameters request (CDPR) bit in a Data Encryption Parameters Complete page set to one;
b) it successfully processes a SECURITY PROTOCOL OUT command, with the SECURITY PROTOCOCOL field set to Tape Data Encryption and with the AUTOMATION COMPLETE RESULTS field in a Data Encryption Parameters Complete page set to a nonzero value; or

c) the data encryption parameters for decryption indicator in the DT device is set to FALSE (e.g., the DT Device includes an SSC-3 compliant device server and has set the data encryption parameters for decryption indicator to FALSE after a data encryption parameters timer has expired).

A key management error (KME) bit set to one indicates that the ERROR TYPE field in the key management error data log parameters (see 6.1.2.5) is set to a non-zero value. If the KME bit is set to one, then the ABT bit shall be set to zero.

The ADC device server shall set the KME bit to zero when the ERROR TYPE field in the key management error data log parameter is set to zero.

If the encryption parameters request (EPR) bit is set to one or the decryption parameters request (DPR) bit is set to one, and the KME bit is set to one, then the automation application client should process the key management error before processing the encryption parameters request.

The ADC device server shall set the abort (ABT) bit to one when the DT device notifies the ADC device server that the data encryption parameters request associated with the value in the PARAMETERS REQUEST SEQUENCE IDENTIFIER field has been aborted.

If the ABT bit is set to one, then the automation application client should abort processing the data encryption parameters request associated with the value in the PARAMETERS REQUEST SEQUENCE IDENTIFIER field. An ABT bit set to one shall not affect the current set of data encryption parameters. If the ABT bit is set to one, then:

a) the encryption parameters request (EPR) bit shall be set to zero;
b) the decryption parameters request (DPR) bit shall be set to zero; and
c) the key management error (KME) bit shall be set to zero.

The ADC device server shall set the ABT bit to zero upon successful completion of a SECURITY PROTOCOL OUT command specifying the Tape Data Encryption security protocol and the Data Encryption Parameters Complete page with the clear abort (CABT) bit set to one.

The automation application client may support aborting processing of data encryption parameters requests. If the ABT bit is set to one, and the application client supports aborting processing of data encryption parameters requests, then the automation application client shall send a SECURITY PROTOCOL OUT command specifying the Tape Data Encryption security protocol and the Data Encryption Parameters Complete page with a data encryption parameters request sequence identifier that matches the sequence identifier value in the PARAMETERS REQUEST SEQUENCE IDENTIFIER field and the CABT bit set to one when:

a) the automation application client processes the abort event and aborts processing the data encryption parameters request with the data encryption parameters request sequence identifier that matches the value in the PARAMETERS REQUEST SEQUENCE IDENTIFIER field; or
b) the automation application client attempts to process the abort event and there is no matching data encryption parameters request sequence identifier (e.g., the automation application client completed processing the data encryption parameters request before starting to process the abort event).

If the ABT bit is set to one and the automation application client does not process the data encryption parameters abort event, then the ABT bit remains set until:

a) the next data encryption parameters request; or
b) a hard reset condition.

The PARAMETERS REQUEST SEQUENCE IDENTIFIER field shall contain the data encryption parameters request sequence identifier:

a) for the data encryption parameters for encryption request if the encryption parameters request (EPR) bit is set to one;
b) for the data encryption parameters for decryption request if the decryption parameters request (DPR) bit is set to one; or
c) for the data encryption parameters request that has been aborted by the ADC device server if the ABT bit is set to one.

The data encryption parameters request sequence identifier shall be a value assigned by the ADC device server that uniquely identifies the data encryption parameters request.

The PARAMETERS REQUEST SEQUENCE IDENTIFIER field shall be ignored if:

a) the key management error (KME) bit is set to one;
b) the encryption parameters request (EPR) bit is set to zero;
c) the decryption parameters request (DPR) bit is set to zero; and
d) the abort (ABT) bit is set to zero.

The DT device ADC data encryption control status log parameter shall not be changed with the use of a LOG SELECT command.

6.1.2.5 Key management error data log parameter

If the key management error (KME) bit is set to one in the DT device ADC data encryption control status log parameter, then the key management error data log parameter shall contain valid information pertaining to the error that caused the KME bit to be set to one. The key management error log parameter format is shown in table 23.

Table 23 — Key management error data log parameter (part 1 of 2)

Bit / Byte	7	6	5	4	3	2	1	0
0	(MSB)							
1	PARAMETER CODE (0003h)							(LSB)
2	DU (0)	DS (1)	TSD (0)	ETC (0)	TMC (00)		LBIN (1)	LP (1)
3	PARAMETER LENGTH (0Ch)							
4	ERROR TYPE				KTO	Reserved		
5	Reserved							
6	(MSB)							
9	PARAMETERS REQUEST ERROR SEQUENCE IDENTIFIER							(LSB)
10	Reserved				SENSE KEY			

Table 23 — Key management error data log parameter (part 2 of 2)

Bit / Byte	7	6	5	4	3	2	1	0
11	ADDITIONAL SENSE CODE							
12	ADDITIONAL SENSE CODE QUALIFIER							
13	Reserved							
15								

The PARAMETER CODE field shall be set to 0003h to indicate the key management error data log parameter.

See SPC-3 for descriptions of the DU bit, DS bit, TSD bit, ETC bit, TMC field, LBIN bit, and LP bit. These bits and fields shall be set to the values shown in table 23.

The PARAMETER LENGTH field shall be set to 0Ch.

The key timeout (KTO) bit set to one indicates that the data encryption period timer expired indicator in the DT device is set to TRUE. The KTO bit set to zero indicates that the encryption parameters period expired indicator in the DT device is set to FALSE. The KTO bit shall be set to zero:

a) if the event that caused the key management error (KME) bit to be set to one in the DT device ADC data encryption control status log parameter was not caused by an encryption parameters period expired indicator in the DT device; or
b) upon successfully processing a SECURITY PROTOCOL OUT command specifying the Tape Data Encryption security protocol and the Data Encryption Parameters Complete page with the clear key management error (CKME) bit set to one.

The ERROR TYPE field indicates the type of the last key management error event (see 4.10.4.5). The error types defined for the ERROR TYPE field are shown in table 24.

Table 24 — ERROR TYPE field

Code	Description
0000b	No error
0001b	encryption parameters request error
0010b	decryption parameters request error
0011b - 1011b	Reserved
1100b - 1111b	Vendor specific

The ADC device server shall set the ERROR TYPE field to zero following successful completion of:

a) an unload operation;
b) a SECURITY PROTOCOL OUT command specifying the Data Encryption Configuration security protocol and the Configure Encryption Policy page;
c) a SECURITY PROTOCOL OUT command specifying the Tape Data Encryption security protocol and the Data Encryption parameters complete page with the clear key management error (CKME) bit set to one; or
d) a hard reset condition (see SAM-3).

The PARAMETERS REQUEST ERROR SEQUENCE IDENTIFIER field shall contain the data encryption parameters request sequence identifier assigned by the ADC device server that uniquely identifies the data encryption parameters request associated with the last key management error event.

See SPC-3 for descriptions of the SENSE KEY field, ADDITIONAL SENSE CODE field, and ADDITIONAL SENSE CODE QUALIFIER field. The SENSE KEY field, ADDITIONAL SENSE CODE field, and ADDITIONAL SENSE CODE QUALIFIER field shall contain the sense data for the most recent event that caused the KME bit to be set to one in the DT device ADC data encryption control status log parameter.

The key management error data log parameter data shall not be changed with the use of a LOG SELECT command.

If the ERROR TYPE field is set to zero, then the SENSE KEY field, ADDITIONAL SENSE CODE field, and ADDITIONAL SENSE CODE QUALIFIER field are undefined.

6.1.2.6 DT device primary port status log parameter(s)

6.1.2.6.1 DT device primary port status log parameter(s) overview

The DT device primary port status log parameter(s) format is shown in table 25..

Table 25 — DT device primary port status log parameter(s) format

Bit Byte	7	6	5	4	3	2	1	0
0	(MSB)							
1	PARAMETER CODE							(LSB)
2	DU (0)	DS (1)	TSD (0)	ETC (0)	TMC (00)		LBIN (1)	LP (1)
3	PARAMETER LENGTH (n-3)							
4								
n	DT device primary port status data							

The PARAMETER CODE field shall be set to the value of the primary port index for the port (see 4.8.1) plus 0100h.

See SPC-3 for descriptions of the DU bit, DS bit, TSD bit, ETC bit, TMC field, LBIN bit, and LP bit. These bits and fields shall be set to the values shown in table 25.

The PARAMETER LENGTH field contains the length in bytes of DT device primary port status data that follows.

The DT device primary port status data is determined by the protocol of the port with which the parameter is associated. The protocol for each port is reported in the PROTOCOL IDENTIFIER field in the DT Device Primary Port

mode subpage (see 6.2.2.2) by primary port index value. The DT device primary port status data shall be determined by table 26 based on the reported protocol for each primary port.

Table 26 — Port status data format by protocol identifier

Code	Description	Reference
0h	Fibre Channel	6.1.2.6.2
1h	Parallel SCSI	6.1.2.6.3
2h - 5h	Reserved	
6h	SAS Serial SCSI Protocol	6.1.2.6.4
7h - Fh	Reserved	

6.1.2.6.2 Fibre Channel port status data

The format of the DT device primary port status data for a Fibre Channel port is shown in table 27.

Table 27 — Fibre Channel port status data format

Bit / Byte	7	6	5	4	3	2	1	0
0	CURRTOP	CURRENT SPEED			LC	CONFLICT	SIGNAL	PIC
1	(MSB)	CURRENT N_PORT_ID						
3								(LSB)
4		Reserved						
6								
7	Reserved	CURRENT FC-AL LOOP ID						
8		CURRENT PORT NAME						
15								
16		CURRENT NODE NAME						
23								

A current topology (CURRTOP) bit set to one indicates that the DT device primary port is operating currently in point to point mode. A CURRTOP bit set to zero indicates that the DT device primary port is operating currently in arbitrated loop mode. The CURRTOP bit shall be ignored when the PIC bit is set to zero.

The CURRENT SPEED field indicates the bit rate at which the DT device primary port is currently operating. Table 48 defines the valid values for the CURRENT SPEED field. The CURRENT SPEED field shall be ignored when the PIC bit is set to zero.

A login complete (LC) bit set to one indicates that at least one initiator port has completed Process Login (see FCP-3) with the DT device on the DT device primary port. A LC bit set to zero indicates that a login has not successfully completed through the PRLI phase on the DT device primary port.

A CONFLICT bit set to one indicates that another device has the required Hard AL_PA (see FC-AL-2) or that no AL_PA is available for the DT device primary port. A CONFLICT bit set to zero indicates there is no AL_PA conflict.

A SIGNAL bit set to one indicates that a signal is detected at the DT device primary port (e.g., detection of light for an optical medium). A SIGNAL bit set to zero indicates a signal is not detected.

A port initialization complete (PIC) bit set to one indicates that the FC_Port state machine is in the ACTIVE state (see FC-FS) and the DT device primary port is operating in point-to-point topology, or the most recent Loop Initialization Process (LIP) has completed successfully (see FC-AL-2). A PIC bit set to zero indicates that the DT device primary port is not in the ACTIVE state and is not synchronized (see FC-FS), or has not successfully completed the most recent LIP.

The CURRENT N_PORT_ID field indicates the 24-bit N_Port_ID (see FC-FS) that is assigned to the DT device primary port. The CURRENT N_PORT_ID field shall be ignored when the PIC bit is set to zero.

The CURRENT FC-AL LOOP ID field indicates the loop identifier (see FC-AL-2) that is assigned to the DT device primary port. The CURRENT FC-AL LOOP ID field shall be ignored when the PIC bit is set to zero or when the CURRTOP bit is set to one.

The CURRENT PORT NAME field contains the DT device's primary port name identifier (see FC-FS).

The CURRENT NODE NAME field contains the DT device's primary node name identifier (see FC-FS).

6.1.2.6.3 SCSI parallel interface port status data

The format of the DT device primary port status data for a SCSI port that supports parallel transfers (see SPI-5) is shown in table 28.

Table 28 — SCSI parallel interface port status data format

Bit / Byte	7	6	5	4	3	2	1	0
0	Reserved					CURRENT BUS MODE		Reserved
1	Reserved							
2	MOST RECENT TRANSFER PERIOD FACTOR							
3	CURRENT SCSI ADDRESS							

The CURRENT BUS MODE field indicates the bus mode in which the DT device primary port is operating (see SPI-5).

The MOST RECENT TRANSFER PERIOD FACTOR field indicates the transfer period factor that was negotiated most recently (see SPI-5).

The CURRENT SCSI ADDRESS field indicates the 8-bit address that is assigned to the DT device primary port.

6.1.2.6.4 Serial Attached SCSI port status data

The format of the DT device primary port status data for a SAS port (see SAS-1.1) is shown in table 29.

Table 29 — Serial Attached SCSI port status data format

Bit / Byte	7	6	5	4	3	2	1	0
0	NEGOTIATED PHYSICAL LINK RATE				Reserved		SIGNAL	PIC
1	(MSB)							
2	HASHED SAS ADDRESS							
3								(LSB
4	(MSB)							
5	SAS ADDRESS							
11								(LSB)

The NEGOTIATED PHYSICAL LINK RATE field indicates the negotiated physical link rate (see SAS-1.1) for at least one phy (see SAS-1.1) that composes the SAS port.

If the port supports the capability to detect signal at the DT device primary port (e.g., COMINIT detected, see SAS-1.1), then a SIGNAL bit set to one indicates that a signal is detected by at least one phy that composes the SAS port. A SIGNAL bit set to zero indicates a signal is not detected by at least one phy that composes the SAS port. If the port does not support the capability to detect signal at the DT device primary port, then the SIGNAL bit shall be set to the value of the PIC bit.

A port initialization complete (PIC) bit set to one indicates that the port has successfully completed the link reset sequence (see SAS-1.1) for at least one phy that composes the SAS port. When port initialization is complete the SAS port is ready to accept connection requests.

The HASHED SAS ADDRESS field contains the hashed version of the SAS address (see SAS-1.1) of the SAS port assigned to the DT device primary port.

The SAS ADDRESS field contains the SAS address (see SAS-1.1) of the SAS port assigned to the DT device primary port.

6.1.3 TapeAlert Response log page

Table 30 describes the TapeAlert Response log page. The parameter fields represent the various TapeAlert state flags (see 4.6). Table 5 contains a description of the corresponding TapeAlert state flags and the conditions that set each state flag to zero.

Table 30 — TapeAlert Response log page

Bit / Byte	7	6	5	4	3	2	1	0
0	Reserved		PAGE CODE (12h)					
1	Reserved							
2	(MSB)		PAGE LENGTH (000Ch)					
3								(LSB)
4	(MSB)		PARAMETER CODE (0000h)					
5								(LSB)
6	DU (0)	DS (1)	TSD (1)	ETC (0)	TMC (00)		LBIN (1)	LP (1)
7	PARAMETER LENGTH (08h)							
8	FLAG01	FLAG02	FLAG03	FLAG04	FLAG05	FLAG06	FLAG07	FLAG08
9	FLAG09	FLAG10	FLAG11	FLAG12	FLAG13	FLAG14	FLAG15	FLAG16
10	FLAG17	FLAG18	FLAG19	FLAG20	FLAG21	FLAG22	FLAG23	FLAG24
11	FLAG25	FLAG26	FLAG27	FLAG28	FLAG29	FLAG30	FLAG31	FLAG32
12	FLAG33	FLAG34	FLAG35	FLAG36	FLAG37	FLAG38	FLAG39	FLAG40
13	FLAG41	FLAG42	FLAG43	FLAG44	FLAG45	FLAG46	FLAG47	FLAG48
14	FLAG49	FLAG50	FLAG51	FLAG52	FLAG53	FLAG54	FLAG55	FLAG56
15	FLAG57	FLAG58	FLAG59	FLAG60	FLAG61	FLAG62	FLAG63	FLAG64

See SPC-3 for a description of the PAGE CODE field.

The PAGE LENGTH field shall be set to 000Ch to allow the transfer of the complete log page.

The PARAMETER CODE field shall be set to 0000h to indicate the single log parameter.

See SPC-3 for descriptions of the DU bit, DS bit, TSD bit, ETC bit, TMC field, LBIN bit, and LP bit. These bits and fields shall be set to the values shown in table 30.

The PARAMETER LENGTH field shall be set to 08h to allow transfer of the complete parameter.

A FLAGXX bit set to one indicates the TapeAlert state flag is set. A FLAGXX bit set to zero indicates the TapeAlert state flag is not set.

6.1.4 Requested Recovery log page

6.1.4.1 Requested Recovery log page overview

Table 31 describes the Requested Recovery log page. When the DT device is unable to complete an action (e.g., a medium load or unload) the DT device may set the RRQST bit to one in the very high frequency data log parameter (see 6.1.2.2) to request that the automation device perform a recovery action. The application client is able to obtain a list of alternative requested recovery actions by reading the Requested Recovery log page.

Table 31 — Requested Recovery log page

Bit / Byte	7	6	5	4	3	2	1	0
0	Reserved		PAGE CODE (13h)					
1	Reserved							
2	(MSB)		PAGE LENGTH (n-3)					
3								(LSB)
4	Requested recovery log parameters							
n								

See SPC-3 for a description of the PAGE CODE field and the PAGE LENGTH field.

Table 32 defines the Requested Recovery log page parameter codes.

Table 32 — Requested Recovery log page parameter codes

Parameter code	Description	Reference
0000h	Recovery procedures	6.1.4.2
0001h - 7FFFh	Reserved	
8000h - FFFFh	Vendor-specific	

6.1.4.2 Recovery procedures log parameter

The recovery procedures log parameter format is shown in table 33.

Table 33 — Requested recovery log parameter format

Bit / Byte	7	6	5	4	3	2	1	0
0	(MSB)							
1	PARAMETER CODE (0000h)							(LSB)
2	DU (1)	DS (1)	TSD (1)	ETC (0)	TMC (00)		LBIN (1)	LP (1)
3	PARAMETER LENGTH (n-3)							
	Recovery procedures list							
4	First recovery procedure							
	. . .							
n	Last recovery procedure							

See SPC-3 for descriptions of the DU bit, DS bit, TSD bit, ETC bit, TMC field, LBIN bit, and LP bit. These bits and fields shall be set to the values shown in table 33.

The PARAMETER LENGTH field indicates the number of recovery procedure bytes that follow.

The PARAMETER CODE field shall be set to 0000h to indicate the recovery procedures log parameter.

The recovery procedures list contain recovery procedures (see table 34) listed in order from the most preferred to the least preferred procedure. When multiple recovery procedures are available, the most preferred procedure shall be the first in the list (i.e., in byte 4), and the other procedures listed in decreasing order of preference. The automation device may select any recovery procedure, regardless of position in the list.

Each recovery procedure consists of one or more actions to be performed. When the INXTN bit in the VHF data descriptor (see 6.1.2.2) is set to one, the parameter shall report only code 00h (i.e., Recovery not requested). If a failure occurs in performing one of the actions in a procedure, then an appropriate list of requested recovery procedures may be reported.

Recovery procedures do not persist across a power cycle.

Table 34 — Recovery procedures

Recovery Procedure	Description
00h	Recovery not requested
01h	Recovery requested, no recovery procedure defined
02h	Push medium
03h	Remove and re-insert medium
04h	Issue a command to unload the medium, then remove and re-insert the medium
05h	Cycle power to DT device
06h	Issue a command to load the medium
07h	Issue a command to unload the medium
08h	Issue LOGICAL UNIT RESET task management function
09h	No recovery procedure defined. Contact service organization
0Ah	Issue a command to unload the medium, then remove and quarantine the medium
0Bh	Do not insert medium. Contact service organization
0Ch	Issue a command to unload the medium, then remove medium and contact service organization
0Dh	Request creation of a DT device error log
0Eh	Retrieve a DT device error log
0Fh	Modify configuration to allow microcode update (see 6.2.2.3.2) and re-insert medium.
10h – 7Fh	Reserved
80h – FFh	Vendor-specific procedures

If the Requested Recovery log page is requested when the RRQST bit n the VHF data descriptor (see 6.1.2.2) is set to zero, then a recovery procedure of 00h (i.e., Recovery not requested) shall be reported.

If the requested recovery procedure causes the DT device to eject the medium, then the automation device shall ensure there is not conflict between the motion of a medium transport element and the medium before initiating that recovery action.

If the requested recovery procedure is 09h (i.e., Contact service organization), then the automation device shall not issue a load or unload command or attempt to manipulate the medium physically.

If the requested recovery procedure is 0Ah (i.e., Issue a command to unload the medium, then remove and quarantine medium), then the medium should not be loaded in a DT device.

If the requested recovery procedure is 0Bh (i.e., Do not insert medium), then a non-recoverable error has occurred and insertion of a medium may cause damage. If the 0Bh recovery procedure is requested, then the RAA bit n the VHF data descriptor shall be set to zero, and no other recovery procedures shall be reported.

If the requested recovery procedure is 0Ch (i.e., issue a command to unload the medium, then remove medium and contact service organization), then a non-recoverable error has occurred and insertion of a new medium may cause damage. When recovery procedure 0Ch is requested and the medium has been removed, then the RAA bit n the VHF data descriptor (see 6.1.2.2) shall be set to zero, and no other recovery procedures shall be reported.

6.1.5 Service Buffers Information log page

The Service Buffers Information log page (see table 35) describes the vendor-specific service buffers (see 6.1.4.2) that are available from the ADC device server that may be retrieved via a READ BUFFER command (see SPC-3). Using the assigned buffer ID, an application client is able to use descriptor mode (see SPC-3) to retrieve the size of the service buffer. An application client is able to use data mode (see SPC-3) to retrieve the service buffer according to the allowable service buffer retrieval conditions provided by the log parameter.

An ADC device server that implements the Service Buffers Information log page shall implement one or more log parameters. Each implemented log parameter shall represent a unique service buffer. Parameters shall not be changed via a LOG SELECT command.

An ADC device server shall save a copy of a service buffer (e.g., a snapshot) in response to:

a) vendor-specific events; or
b) processing a READ BUFFER command using descriptor mode with the BUFFER ID field set to a value that matches the BUFFER ID field value of one of the service buffers described by a parameter of the Service Buffers Information log page for which an unread copy of the service buffer does not exist.

An ADC device server that implements the Service Buffers Information log page should indicate Retrieve a DT device error log (see table 34) in the recovery procedures when a copy of a service buffer of any service buffer exists. The copy of a service buffer should be maintained until the service buffer associated with the buffer ID in the READ BUFFER command is completely read. The copy of the service buffer may be cleared on a:

c) vendor-specific event;
d) LOGICAL UNIT RESET;
e) TARGET RESET; or
f) POWER ON RESET.

Table 35 — Service Buffers Information log page

Bit / Byte	7	6	5	4	3	2	1	0
0	Reserved		PAGE CODE (15h)					
1	Reserved							
2	(MSB)		PAGE LENGTH (n-3)					
3								(LSB)
4	Service buffers information log parameters							
n								

See SPC-3 for a description of the PAGE CODE field and the PAGE LENGTH field.

The service buffer information log parameter format is shown in table 36.

Table 36 — Service buffer information log parameter format

Bit / Byte	7	6	5	4	3	2	1	0
0	(MSB)							
1				PARAMETER CODE				(LSB)
2	DU (0)	DS (1)	TSD (1)	ETC (0)	TMC (00)		LBIN (1)	LP (1)
3	PARAMETER LENGTH (n-3)							
4	BUFFER ID							
5	Reserved			TU	NMP	NMM	OFFLINE	PD
6	Reserved				CODE SET			
7	Reserved							
8				SERVICE BUFFER TITLE				
n								

The PARAMETER CODE field is defined in table 37.

Table 37 — Service buffer information parameter codes

Code	Description
0000h - 00FFh	Service buffer identifier
0100h - 7FFFh	Reserved
8000h - FFFFh	Vendor-specific

See SPC-3 for descriptions of the DU bit, DS bit, TSD bit, ETC bit, TMC field, LBIN bit, and LP bit. These bits and fields shall be set to the values shown in table 36.

The PARAMETER LENGTH field contains the length in bytes of service buffer information data that follows.

See SPC-3 for a description of the BUFFER ID field.

The TU bit, NMP bit, NMM bit, OFFLINE bit, and PD bit are collectively referred to as the service buffer retrieval control byte, and are described in this subclause.

A temporarily unavailable (TU) bit set to one indicates that the service buffer identified by the contents of the BUFFER ID field is temporarily unavailable for retrieval from the device server for reasons outside the scope of this standard. A TU bit set to zero indicates that the service buffer identified by the contents of the BUFFER ID field is able to be retrieved from the device server.

A no medium present (NMP) bit set to one indicates that the device server is unable to retrieve the service buffer identified by the contents of the BUFFER ID field when a medium is present in the DT device (see 4.4). A NMP bit set to zero indicates that the device server is able to retrieve the service buffer identified by the contents of the BUFFER ID field when a medium is present in the DT device.

A no medium mounted (NMM) bit set to one indicates that the device server is unable to retrieve the service buffer identified by the contents of the BUFFER ID field when a medium is mounted in the DT device (see 4.4). A NMM bit set to zero indicates that the device server is able to retrieve the service buffer identified by the contents of the BUFFER ID field when a medium is mounted in the DT device.

An OFFLINE bit set to one indicates that the device server is unable to retrieve the service buffer identified by the contents of the BUFFER ID field when the RMC device server is online (see 6.2.2.3.2). An OFFLINE bit set to zero indicates that the device server is able to retrieve the service buffer identified by the contents of the BUFFER ID field when the RMC device server is online.

A port disabled (PD) bit set to one indicates that the device server is unable to retrieve the service buffer identified by the contents of the BUFFER ID field is when the DT device primary port(s) associated with the RMU logical unit are enabled (see 6.2.2.2.2). A PD bit set to zero indicates that the device server is able to retrieve the service buffer identified by the contents of the BUFFER ID field when the DT device primary port(s) associated with the RMU logical unit are enabled.

See SPC-3 for a description of the CODE SET field.

The SERVICE BUFFER TITLE field contains ASCII information describing the service buffer identified by the contents of the BUFFER ID field. The data in this field shall be formatted as a single character string line and shall contain only graphic codes (i.e., code values 20h through 7Eh) and shall be terminated with a NULL (00h) character.

6.2 Mode parameters

6.2.1 Mode parameters overview

This subclause defines the descriptors and pages for mode parameters used with ADC device servers.

See SPC-3 for a description of the mode parameter list, including the mode parameter header and mode block descriptor.

The MEDIUM TYPE field in the mode parameter header is reserved for ADC device servers.

The DEVICE-SPECIFIC PARAMETER field in the mode parameter header is reserved for ADC device servers.

The DENSITY CODE field in the mode parameter block descriptor is reserved for ADC device servers.

The ADC device server may require that the DT device primary port(s) be disabled before certain mode parameters are allowed to be changed (see 6.2.2.2).

The mode page codes for ADC device servers are shown in table 38.

Table 38 — Mode page codes

Page code	Subpage code	Description	Reference
02h	00h	Disconnect-Reconnect mode page	SPC-3
0Ah	00h	Control mode page	SPC-3
0Ah	01h	Control Extension page	SPC-3
0Eh	01h	Target Device subpage [b]	6.2.2.1
0Eh	02h	DT Device Primary Port subpage [b]	6.2.2.2
0Eh	03h	Logical Unit subpage [b]	6.2.2.3
0Eh	04h	Target Device Serial Number subpage [b]	6.2.2.4
15h	00h	Restricted	
18h	00h	Protocol Specific LUN mode page	SPC-3
18h	01h - FEh	(see specific SCSI transport protocol)	SPC-3
19h	00h	Protocol Specific Port mode page	SPC-3
19h	01h - FEh	(see specific SCSI transport protocol)	SPC-3
1A	00h	Power Condition page	SPC-3
1Ch	00h	Informational Exceptions Control mode page	SSC-3
20h - 3Eh	00h - FEh	Vendor-specific	
01h - 3Eh	FFh	Return all subpages [a]	SPC-3
3Fh	00h	Return all pages [a]	SPC-3
3Fh	FFh	Return all pages and subpages [a]	SPC-3

All page code and subpage code combinations not shown in this table are reserved.

[a] valid only for the MODE SENSE (see SPC-3) command.

[b] This subpage contains one or more descriptors. The descriptors may be included in any order. On a MODE SENSE command, all descriptors supported by the ADC device server shall be returned. On a MODE SELECT command (see SPC-3), all of the supported descriptors shall be included. Any descriptor included shall be included in its entirety.

6.2.2 ADC Device Server Configuration mode page

6.2.2.1 Target Device subpage

The Target Device subpage is variable length and contains SCSI target device name identification descriptors (see SPC-3) of the DT device. The subpage is defined in table 39.

Table 39 — Target Device subpage

Bit / Byte	7	6	5	4	3	2	1	0
0	PS	SPF (1b)	PAGE CODE (0Eh)					
1	SUBPAGE CODE (01h)							
2	(MSB)	PAGE LENGTH (n-3)						
3								(LSB)
4	Reserved						MTDN	
5	Reserved							
6	Reserved							
7	Reserved							
	Identification descriptor list							
8	Identification descriptor (first)							
	.							
	.							
	Identification descriptor (last)							
n								

See SPC-3 for a description of the PS bit, SPF bit, PAGE CODE field, SUBPAGE CODE field, and PAGE LENGTH field. The SPF bit, PAGE CODE field, and SUBPAGE CODE field shall be set to the values shown in table 39.

The modify target device name (MTDN) field and identification descriptors are used to modify and report modifications to the DT device SCSI target device names (see SPC-3), as defined in table 40.

Table 40 — MTDN field

Value	MODE SENSE command [a]	MODE SELECT command [a]
00b	The MTDN field shall be set to zero for a MODE SENSE command. The identification descriptors shall contain the currently assigned values.	Do not modify the DT device's SCSI target device names. The identification descriptors shall be ignored.
01b	Invalid	Use the logical unit identifier for LUN 0 as the DT device SCSI target device name. The identification descriptors shall be ignored.
10b		Set the DT device's SCSI target device names to the manufacturer's default value. The identification descriptors shall be ignored.
11b		Set the DT device's SCSI target device names to the values in the identification descriptors.
[a] See SPC-3.		

The identification descriptors are the same as those in the Device Identification VPD page (see SPC-3). Only identification descriptors with the ASSOCIATION field set to 10b (i.e., target device) shall be used. On MODE SELECT commands, if any identification descriptor contains an ASSOCIATION field set to a value other than 10b, then the ADC device server shall return CHECK CONDITION status, setting the sense key to ILLEGAL REQUEST and the additional sense code to INVALID FIELD IN PARAMETER LIST.

A device server processing a MODE SELECT command with parameter data containing the Target Device subpage and the MTDN field set to 01b shall not modify the DT device's SCSI target device name and shall return CHECK CONDITION status with the sense key set to ILLEGAL REQUEST and the additional sense code set to INVALID FIELD IN PARAMETER LIST if:

a) the DT device supports multiple primary ports;
b) a transport protocol for a primary port in the DT device mandates uniqueness of the SCSI target device name and the name of a SCSI logical unit within the DT device; or
c) a transport protocol for a primary port in the DT device mandates a name format for the SCSI target device name that differs from the name format of all of the logical unit identifiers of LUN 0.

6.2.2.2 DT Device Primary Port subpage

6.2.2.2.1 DT Device Primary Port subpage overview

The DT Device Primary Port subpage contains descriptors that allow the DT device's primary ports to be configured, independent of the port type receiving the command (e.g., a Fibre Channel DT device primary port may be configured via the DT device's ADI port).

The DT Device Primary Port subpage is variable length, and consists of a mode subpage header followed by one or more descriptors (see table 41).

Table 41 — DT Device Primary Port subpage

Bit / Byte	7	6	5	4	3	2	1	0
0	PS	SPF (1b)	PAGE CODE (0Eh)					
1	SUBPAGE CODE (02h)							
2	(MSB)		PAGE LENGTH (n-3)					
3								(LSB)
	DT device primary port descriptor list							
4			DT device primary port descriptor (first)					
			.					
			.					
			DT device primary port descriptor (last)					
n								

See SPC-3 for a description of the PS bit, SPF bit, PAGE CODE field, SUBPAGE CODE field, and PAGE LENGTH field. The SPF bit, PAGE CODE field, and SUBPAGE CODE field shall be set to the values shown in table 41.

6.2.2.2.2 DT device primary port descriptor format

The DT device primary port descriptor format is shown in table 42.

Table 42 — DT device primary port descriptor format

Bit / Byte	7	6	5	4	3	2	1	0
0	PRIMARY PORT INDEX							
1	Reserved				PROTOCOL IDENTIFIER			
2	(MSB)		ADDITIONAL DESCRIPTOR LENGTH (n-3)					
3								(LSB)
4			DT device primary port descriptor parameters					
n								

The PRIMARY PORT INDEX field contains the primary port index (see 4.8.1) assigned by the DT device.

The PROTOCOL IDENTIFIER field indicates the type of protocol supported by the DT device primary port (see SPC-3). For the MODE SELECT command, if the protocol identifier specified by the PROTOCOL IDENTIFIER field does not match the protocol of the target port specified by the PRIMARY PORT INDEX field, the device server shall terminate the command with CHECK CONDITION status with the sense key set to ILLEGAL REQUEST and the additional sense code set to INVALID FIELD IN PARAMETER LIST.

The ADDITIONAL DESCRIPTOR LENGTH field specifies the number of descriptor bytes that follow.

The DT device primary port descriptors vary based on the value in the PROTOCOL IDENTIFIER field (see table 43).

Table 43 — Primary port descriptor by protocol identifier value

Value	Description	Reference
0h	Fibre Channel descriptor	6.2.2.2.3
1h	Parallel SCSI descriptor	6.2.2.2.4
2h - 5h	Reserved	
6h	Serial Attached SCSI descriptor	6.2.2.2.5
7h - Fh	Reserved	

6.2.2.2.3 Fibre Channel descriptor parameter format

Table 44 describes the format of the descriptor parameter for Fibre Channel port types.

Table 44 — Fibre Channel descriptor parameter format

Byte \ Bit	7	6	5	4	3	2	1	0
0	P2P	TOPLOCK	RHA	LIV	MPN		Rsvd	PE
1	Reserved			TOPORD	SPDLOCK	SPEED		
2	Reserved							
3	Rsvd	FC-AL LOOP ID						
4	PORT NAME							
11								

A DT device receiving a MODE SELECT command (see SPC-3) for an enabled DT device primary port, where the command attempts to change the value of the MPN field, LIV bit, RHA bit, TOPLOCK bit, P2P bit, SPEED field, SPDLOCK bit, TOPORD bit, FC-AL LOOP ID field, or PORT NAME field, shall return CHECK CONDITION status with the sense key set to ILLEGAL REQUEST and the additional sense code set to INVALID FIELD IN PARAMETER LIST. If the DT device primary port is disabled, then the DT device may change the MPN field, LIV bit, RHA bit, TOPLOCK bit, P2P bit, SPEED field, SPDLOCK bit, FC-AL LOOP ID field, or PORT NAME field and enable the DT device primary port with the same MODE SELECT command.

The point-to-point (P2P) bit, topology order (TOPORD) bit, and topology lock (TOPLOCK) bit define the method by which the DT device primary port connects to the service delivery subsystem. Table 45 defines how the TOPLOCK bit, P2P bit, and TOPORD bit interact.

Table 45 — TOPLOCK bit, P2P bit, and TOPORD bit interaction

TOPLOCK	TOPORD	P2P	Description
0	0	x	Vendor-specific behavior for negotiating topology (see FC-FS).
0	1	0	The port attempts to negotiate operation in FC-AL topology first. If unsuccessful, then the port negotiates operation in point-to-point mode.
0	1	1	The port attempts to negotiate operation in point-to-point mode first. If unsuccessful then negotiates to FC-AL topology.
1	x	0	The port is configured to operate in arbitrated loop mode.
1	x	1	The port is configured to operate in point-to-point mode and the RHA bit, LIV bit, and FC-AL LOOP ID field shall be ignored in a MODE SELECT command.

The loop ID valid (LIV) bit and require hard address (RHA) bit are described in table 46.

Table 46 — Effect of LIV and RHA bits

LIV	RHA	Description
0b	0b	The FC-AL LOOP ID field shall be ignored.
0b	1b	This bit value combination is invalid. A MODE SELECT command (see SPC-3) shall be terminated with a CHECK CONDITION status. The sense key shall be set to ILLEGAL REQUEST and the additional sense code shall be set to INVALID FIELD IN PARAMETER LIST.
1b	0b	The DT device primary port attempting to operate in an arbitrated loop topology shall use the value in the FC-AL LOOP ID field to request the Hard AL_PA during the LIHA Loop Initialization Sequence (see FC-AL-2) provided it has not already obtained its address. The DT device primary port may obtain its address during any of the Loop Initialization Sequences.
1b	1b	The DT device primary port attempting to operate in an arbitrated loop topology shall use the value in the FC-AL LOOP ID field to obtain its address during the LIHA Loop Initialization Sequence. The DT device primary port shall not obtain an address during the LIFA or LIPA Loop Initialization Sequences if the value of the FC-AL LOOP ID field does not match the previously obtained address. The DT device primary port shall not attempt to obtain an address during the LISA Loop Initialization Sequence. If there is a conflict for the Hard Address (see FC-AL-2) during loop initialization, then the DT device primary port shall enter the nonparticipating state. If the DT device primary port detects loop initialization while in the nonparticipating state, then the DT device primary port shall again attempt to get the address specified by the value in the FC-AL LOOP ID field.

The modify port name (MPN) field and PORT NAME field are used to modify and report modifications to the DT device primary port's name identifier (see FC-FS), as defined in table 47.

Table 47 — MPN field

Code	MODE SENSE command [a]	MODE SELECT command [a]
00b	The MPN field shall be set to zero for a MODE SENSE command. The PORT NAME field shall contain the currently assigned value.	Do not modify the DT device primary port's name identifier (see FC-FS). The PORT NAME field shall be ignored.
01b	Invalid	Reserved.
10b		Set the DT device primary port's name identifier to the manufacturer's default value. The value in the PORT NAME field shall be ignored.
11b		Set the DT device primary port's name identifier to the value in the PORT NAME field.
[a] See SPC-3.		

A port enable (PE) bit set to one enables the DT device primary port (see 4.8). When the PE bit is set to zero, the DT device shall not enable the DT device primary port's drivers and the DT device primary port shall not respond to primitives (see FC-AL-2).

A speed lock (SPDLOCK) bit set to one forces the DT device primary port to only operate in the speed selected by the SPEED field. A SPDLOCK bit set to zero allows the DT device primary port to negotiate the speed (see FC-FS). When the SPDLOCK bit is set to zero on a MODE SELECT command, the SPEED field shall be ignored.

The SPEED field contains the bit rate in which the DT device primary port is configured to operate. Table 48 defines the valid values for the SPEED field.

Table 48 — Fibre Channel speed values

Code	Speed
000b	1 Gb/sec
001b	2 Gb/sec
010b	4 Gb/sec
011b	8 Gb/sec
100b	10 Gb/sec
101b – 111b	Reserved

The FC-AL LOOP ID field contains the loop identifier that shall be used to represent the hard assigned AL_PA (see FC-AL-2).

The PORT NAME field contains the DT device's primary port name identifier (see FC-FS). When the MPN field is set to 11b (see table 47), the PORT NAME field contains an NAA identifier type name identifier (see SPC-3).

6.2.2.2.4 Parallel SCSI descriptor parameter format

Table 49 defines the format of the descriptor parameter for parallel SCSI port types.

Table 49 - Parallel SCSI descriptor parameter format

Bit / Byte	7	6	5	4	3	2	1	0
0	Reserved			BMQ		BUS MODE		PE
1	Reserved							
2	MINIMUM TRANSFER PERIOD FACTOR							
3	SCSI ADDRESS							

A DT device receiving a MODE SELECT command (see SPC-3) for an enabled DT device primary port, where the command attempts to change the value of the BUS MODE field, BMQ field, MINIMUM TRANSFER PERIOD FACTOR field, or SCSI ADDRESS field, shall return CHECK CONDITION status with the sense key set to ILLEGAL REQUEST and the additional sense code set to INVALID FIELD IN PARAMETER LIST. If the DT device primary port is disabled, then the DT device may change the BUS MODE field, BMQ field, MINIMUM TRANSFER PERIOD FACTOR field, or SCSI ADDRESS field and enable the DT device primary port with the same MODE SELECT command.

The bus mode qualifier (BMQ) field (see table 50) qualifies the effect that the BUS MODE field has on the DT device primary port.

Table 50 — BMQ field

Code	Effect
00b	The DT device shall ignore the value of the BUS MODE field.
01b	The DT device operates the DT device primary port as specified by the BUS MODE field. The DT device primary port shall not drive the DIFFSENS line with the associated voltage and current characteristics (see SPI-5).
10b	Reserved
11b	The DT device operates the DT device primary port in the mode specified by the BUS MODE field. The DT device primary port shall drive the DIFFSENS line with the associated voltage and current characteristics (see SPI-5).

The BUS MODE field defines the transmission mode that the DT device shall use in the TRANSCEIVER MODE field of the Negotiated Settings mode subpage (see SPI-5) for this DT device primary port.

A port enable (PE) bit set to one enables the DT device primary port to respond to selections on the SCSI bus (see SPI-5). A PE bit set to zero prevents the DT device primary port from responding to or attempting selections, reselections, or hard resets on the SCSI bus (see 4.8).

The MINIMUM TRANSFER PERIOD FACTOR field defines the minimum transfer period factor that the DT device shall use when negotiating transfer agreements (see SPI-5) for this DT device primary port. DT devices that are not able to support the identified minimum transfer period factor may enter negotiation using the next larger supported transfer period factor.

The SCSI ADDRESS field specifies the address that the DT device primary port shall respond to on the SCSI bus.

6.2.2.2.5 Serial Attached SCSI descriptor parameter format

Table 51 describes the format of the descriptor parameter for SAS port types.

Table 51 — Serial Attached SCSI descriptor parameter format

Bit / Byte	7	6	5	4	3	2	1	0
0	Reserved				MPI		Rsvd	PE
1	Reserved							
3								
4	PORT IDENTIFIER							
11								

A DT device receiving a MODE SELECT command (see SPC-3) for an enabled DT device primary port, where the command attempts to change the port identifier (see table 52), shall return CHECK CONDITION status with the sense key set to ILLEGAL REQUEST and the additional sense code set to INVALID FIELD IN PARAMETER LIST. If the DT device primary port is disabled, then the automation application client may change the DT device port identifier and enable the DT device primary port with the same MODE SELECT command.

The modify port identifier (MPI) field and PORT IDENTIFIER field control the DT device primary SAS port identifier (see SAS-1.1) as defined in the table 52.

Table 52 — MPI field

Code	MODE SENSE command [a]	MODE SELECT command [a]
00b	The MPI field shall be set to zero for a MODE SENSE command. The PORT IDENTIFIER field shall contain the currently assigned port identifier value.	Do not modify the DT device primary port identifier (see SAS-1.1). The PORT IDENTIFIER field shall be ignored.
01b	Invalid	Reserved
10b		Set the DT device primary port identifier to the manufacturer's default value. The value in the PORT IDENTIFIER field shall be ignored.
11b		Set the DT device primary port identifier to the value contained in the PORT IDENTIFIER field.

[a] See SPC-3.

A port enable (PE) bit set to one enables the DT device primary SAS port. When the PE bit is set to zero, the DT device shall not enable any phy contained in the DT device primary SAS port (see SAS-1.1).

The PORT IDENTIFIER field contains the DT device's primary SAS port identifier (see SAS-1.1). When the MPI field is set to 11b, the PORT IDENTIFIER field shall contain an NAA IEEE Registered format identifier (see SAS-1.1).

6.2.2.3 Logical Unit subpage

6.2.2.3.1 Logical Unit subpage overview

The Logical Unit subpage is variable-length, and consists of a mode subpage header followed by one or more descriptors. The descriptors may be included in any order. On a MODE SENSE command (see SPC-3), all logical units supported by the DT device (i.e., ADC logical units, RMC logical units, and SMC logical units) other than W-LUNs (see SPC-3) shall have descriptors returned. On a MODE SELECT command (see SPC-3), all of the supported descriptors shall be included. Any descriptor included shall be included in its entirety.

Table 53 describes the Logical Unit subpage.

Table 53 — Logical Unit subpage

Bit / Byte	7	6	5	4	3	2	1	0
0	PS	SPF (1b)	PAGE CODE (0Eh)					
1	SUBPAGE CODE (03h)							
2	(MSB)							
3	PAGE LENGTH (n-3)							(LSB)
	Logical unit descriptor list							
4	Logical unit descriptor (first)							
	.							
	.							
	Logical unit descriptor (last)							
n								

See SPC-3 for a description of the PS bit, SPF bit, PAGE CODE field, SUBPAGE CODE field, and PAGE LENGTH field. The SPF bit, PAGE CODE field, SUBPAGE CODE field shall be set to the values shown in table 53.

The logical unit descriptors are described in this subclause.

6.2.2.3.2 RMC logical unit descriptor format

The descriptor format for an RMC logical unit (e.g., DEVICE TYPE field contains 01h in the case of a sequential-access device (see SPC-3)) is defined in table 54.

Table 54 — RMC logical unit descriptor format

Bit / Byte	7	6	5	4	3	2	1	0
0	LOGICAL UNIT INDEX							
1	DEVICE TYPE							
2	(MSB)							
3	ADDITIONAL DESCRIPTOR LENGTH (n-3)							(LSB)
4								
5	LOGICAL UNIT NUMBER							
6	MLUD		Reserved				OFFLINE	ENABLE
7	Reserved		AUH	SUHO	AMO	AUTOLOAD MODE		
8	MUE	MUP	Reserved	MANDROFF	CP	DRMODE	Reserved	WP
9	CURRENT DENSITY							
10	Reserved							
11	Reserved							
12	Reserved							
13	Reserved							
14	Reserved							
15	Reserved							
	Identification descriptor list							
16								
	Identification descriptor (first)							
	.							
	.							
n	Identification descriptor (last)							

The LOGICAL UNIT INDEX field contains a value assigned by the DT device at power on that uniquely identifies the RMC logical unit from all other logical units on the DT device, independent of device server. This field shall not be changeable. The ADC device server shall terminate a MODE SELECT command that attempts to change the value in the LOGICAL UNIT INDEX field with CHECK CONDITION status with the sense key to ILLEGAL REQUEST and the additional sense code set to INVALID FIELD IN PARAMETER LIST.

The DEVICE TYPE field defines the type of command set supported by the RMC logical unit. The DEVICE TYPE field contains the same value that would be returned by the RMC logical unit in the PERIPHERAL DEVICE TYPE field for an INQUIRY command (see SPC-3).

The ADDITIONAL DESCRIPTOR LENGTH field specifies the number of descriptor bytes that follow.

The LOGICAL UNIT NUMBER field specifies, for the RMC logical unit when accessed through the DT device primary port(s):

a) the LUN if access controls are not in effect; or
b) the default LUN if access controls are in effect (see SPC-3).

The LOGICAL UNIT NUMBER field contains the first two bytes (i.e., bytes 0 and 1) of a single level logical unit structure or the contents of a two byte extended logical unit address (see SAM-3). The LOGICAL UNIT NUMBER field shall be ignored if the ENABLE bit is set to zero. The ADC device server shall return a CHECK CONDITION status to a MODE SELECT command (see SPC-3) when multiple descriptors with the ENABLE bit set to one have the same value in the LOGICAL UNIT NUMBER field. The sense key shall be set to ILLEGAL REQUEST and the additional sense code shall be set to INVALID FIELD IN PARAMETER LIST.

The modify logical unit descriptor (MLUD) field (see table 55) modifies and reports modifications to the RMC logical unit's device identifiers.

Table 55 — MLUD **field**

Code	MODE SENSE command [a]	MODE SELECT command [a]
00b	The MLUD field shall be set to zero for a MODE SENSE command. The identification descriptors shall contain the currently assigned values.	Do not modify the RMC logical unit's device identifiers. The identification descriptors shall be ignored.
01b	Invalid	Reserved
10b		Set the RMC logical unit's device identifiers to the manufacturer's default values. The identification descriptors shall be ignored.
11b		Set the RMC logical unit's device identifiers to the values in the identification descriptors.

[a] See SPC-3.

If the OFFLINE bit is set to one, then the RMC device server shall return CHECK CONDITION status with the sense key set to NOT READY and the additional sense code set to LOGICAL UNIT NOT READY, OFFLINE to all commands that require the RMC logical unit to be in the ready state. If the OFFLINE bit is set to zero, then the RMC device server shall respond normally to commands.

An ENABLE bit set to one specifies that the DT device primary port(s) associated with the RMC logical unit shall be responsive to commands and task management requests received on the DT device primary port(s). An ENABLE bit set to zero specifies that the DT device primary port(s) associated with the RMC logical unit shall not respond to commands and task management requests received on the DT device primary port(s) and the associated RMC logical unit number shall not be included in the logical unit inventory (see SPC-3) for all I_T nexuses associated with a DT device primary port. The ENABLE bit has no effect on the access to the RMC device server through the ADI port.

If the ENABLE bit is changed from one to zero, then the RMC device server shall implicitly abort all commands in its task set received on a DT device primary port and report CHECK CONDITION status with the sense key set to ABORTED COMMAND and the additional sense code set to LOGICAL UNIT COMMUNICATION FAILURE for each command. All remaining device servers (e.g., local SMC device server, ADC device server) in the DT device shall report a change in the logical unit inventory (see SPC-3) to any application clients connected through a DT

device primary port. The ENABLE bit changing from one to zero shall have no effect on commands and task management requests received on an ADI port.

An automatic unload hold (AUH) bit set to one disables ejecting the medium when the medium is unloaded due to DT device specific conditions (e.g., cleaning complete, invalid medium type, microcode update complete, unsupported format, or other error conditions detected by the DT device). An AUH bit set to zero shall have no effect on the ejecting of the medium. The AUH bit does not affect the unload operation initiated via the physical user interface of the DT device.

A SCSI unload hold override (SUHO) bit set to one specifies the HOLD bit in the LOAD UNLOAD command (see SSC-2) shall be ignored by the RMC device server and the medium shall not be ejected. A SUHO bit set to zero specifies the HOLD bit in the LOAD UNLOAD command shall control if the medium is ejected or not, as processed by the RMC device server. The SUHO bit shall not affect LOAD UNLOAD commands processed by the ADC device server.

An autoload mode override (AMO) bit set to one specifies the load process shall be controlled by the AUTOLOAD MODE field (see table 56), overriding the settings in the Control mode page AUTOLOAD MODE field (see SPC-3). An AMO bit set to zero specifies that the settings in the Control mode page AUTOLOAD MODE field shall be used to control the load process.

The AUTOLOAD MODE field (see table 56) specifies the action to be taken by the DT device when a medium is inserted. If the AMO bit is set to zero, then the AUTOLOAD MODE field shall be ignored.

Table 56 — AUTOLOAD MODE **field**

Code	Definition
000b	Medium shall be loaded for full access.
001b	Medium shall be loaded for medium auxiliary memory access only.
010b	Medium shall not be loaded.
011b – 111b	Reserved

A microcode update enable (MUE) bit set to one allows the DT device to prepare to accept a medium containing a microcode image. A description of this preparation is outside the scope of this standard. The behavior when the MUE bit is set to zero is vendor specific. The MUE bit shall be set to zero by the DT device after the microcode update process completes or is aborted.

A microcode update protect (MUP) bit set to one shall prevent the DT device from performing a microcode update process upon the loading of a medium containing a microcode image. A MUP bit set to zero shall not prevent the DT device from performing a microcode update process upon the loading of a medium containing a microcode image.

A manual disaster recovery off (MANDROFF) bit set to one specifies that the DT device shall exit disaster recovery mode when an application client sets the DRMODE bit to zero. A MANDROFF bit set to zero specifies that the DT device shall exit disaster recovery mode upon detection of a vendor-specific event.

A clean protect (CP) bit set to one shall prevent the DT device from performing a cleaning operation upon the loading of a cleaning medium. A CP bit set to zero shall not prevent the DT device from performing a cleaning operation upon the loading of a cleaning medium.

A disaster recovery mode (DRMODE) bit set to one specifies that the DT device shall operate in disaster recovery mode. A DRMODE bit set to zero specifies that the DT device shall not operate in disaster recovery mode. The

definition of disaster recovery mode is outside the scope of this standard. The ADC device server shall set the DRMODE bit to zero when the MANDROFF bit is set to zero and the DT device exits disaster recovery mode.

A write protect (WP) bit set to one shall enable write protection (see the relevant RMC command standard). A WP bit set to zero shall disable this source of write protection. The WP bit shall be set to zero by the DT device each time a medium is unloaded.

The CURRENT DENSITY field shall be set to the density code associated with the density in which the DT device is currently operating. The CURRENT DENSITY field shall be ignored by the DT device on MODE SELECT commands.

The identification descriptors are the same as those in the Device Identification VPD page (see SPC-3). Only identification descriptors with the ASSOCIATION field set to 00b (i.e., logical unit) shall be used. On MODE SELECT commands, if any identification descriptor contains an ASSOCIATION field set to a value other than 00b, then the ADC device server shall return CHECK CONDITION status with the sense key to ILLEGAL REQUEST and the additional sense code set to INVALID FIELD IN PARAMETER LIST.

6.2.2.3.3 SMC logical unit descriptor format

The descriptor format for an SMC logical unit is defined in table 57.

Table 57 — SMC logical unit descriptor format

Bit Byte	7	6	5	4	3	2	1	0
0	LOGICAL UNIT INDEX							
1	DEVICE TYPE (08h)							
2	(MSB)			ADDITIONAL DESCRIPTOR LENGTH (08h)				
3								(LSB)
4				LOGICAL UNIT NUMBER				
5								
6				Reserved			CACHE	ENABLE
7	Reserved							
8	(MSB)			REMOTE SMC DEVICE SERVER LOGICAL UNIT NUMBER				
9								(LSB)
10				Reserved				
11								

The LOGICAL UNIT INDEX field contains a value assigned by the DT device at power on that uniquely identifies the SMC logical unit from all other logical units on the DT device, independent of device server. This field shall not be changeable. The ADC device server shall terminate a MODE SELECT command that attempts to change the value in the LOGICAL UNIT INDEX field with CHECK CONDITION status with the sense key to ILLEGAL REQUEST and the additional sense code set to INVALID FIELD IN PARAMETER LIST.

The DEVICE TYPE field shall contain the value shown in table 57 (i.e., 08h, a medium changer device (see SPC-3)).

The ADDITIONAL DESCRIPTOR LENGTH field contains the number of descriptor bytes that follow and shall be set to the value shown in table 57.

The LOGICAL UNIT NUMBER field specifies, for the SMC logical unit when accessed through the DT device primary port(s):

a) the LUN if access controls are not in effect; or
b) the default LUN if access controls are in effect (see SPC-3).

The bridging manager shall use the value of the REMOTE SMC DEVICE SERVER LOGICAL UNIT NUMBER field when addressing the automation device logical unit containing the remote SMC device server (see 4.3).

The LOGICAL UNIT NUMBER field and the REMOTE SMC DEVICE SERVER LOGICAL UNIT NUMBER field each contain the first two bytes (i.e., bytes 0 and 1) of a single level logical unit structure or the contents of a two byte extended logical unit address (see SAM-3). The LOGICAL UNIT NUMBER field and the REMOTE SMC DEVICE SERVER LOGICAL UNIT NUMBER field shall be ignored if the ENABLE bit is set to zero. The ADC device server shall return a CHECK CONDITION status with the sense key set to ILLEGAL REQUEST and the additional sense code set to INVALID FIELD IN PARAMETER LIST to a MODE SELECT command (see SPC-3) if multiple descriptors with the ENABLE bit set to one have the same value in the LOGICAL UNIT NUMBER field.

A CACHE bit set to one and the ENABLE bit set to one specifies that the local SMC device server may cache SMC data and status (see 4.3.5). If the ADC device server receives a MODE SELECT command with parameter data of the ENABLE bit set to zero and the CACHE bit set to one, then the ADC device server shall return CHECK CONDITION status with the sense key set to ILLEGAL REQUEST and an additional sense code set to INVALID FIELD IN PARAMETER LIST. A CACHE bit set to zero or an ENABLE bit set to zero specifies that the local SMC device server shall not cache SMC data and status.

An ENABLE bit set to one specifies that the DT device primary port(s) associated with the SMC logical unit shall be responsive to commands and task management requests received on the DT device primary port(s). Received commands may be processed by the local SMC device server or may be passed by the bridging manager to the remote SMC device server for processing (see 4.3). An ENABLE bit set to zero specifies that the DT device primary port(s) associated with the SMC logical unit shall not respond to commands and task management requests received on the DT device primary port(s) and the associated SMC logical unit number shall not be included in the logical unit inventory (see SPC-3) for all I_T nexuses associated with a DT device primary port. The ENABLE bit has no effect on the access to the SMC device server through the ADI port.

If the ENABLE bit is changed from one to zero, then the local SMC device server shall implicitly abort all commands in its task set and report CHECK CONDITION status with the sense key set to ABORTED COMMAND and the additional sense code set to LOGICAL UNIT COMMUNICATION FAILURE for each command. All remaining device servers (e.g., ADC device server, RMC device server) in the DT device shall report a change in the logical unit inventory (see SPC-3) to any application clients connected through a DT device primary port.

6.2.2.3.4 ADC logical unit descriptor format

The descriptor format for an ADC logical unit is defined in table 58.

Table 58 — ADC logical unit descriptor format

Bit / Byte	7	6	5	4	3	2	1	0
0	LOGICAL UNIT INDEX							
1	DEVICE TYPE (12h)							
2	(MSB)			ADDITIONAL DESCRIPTOR LENGTH (04h)				
3								(LSB)
4				LOGICAL UNIT NUMBER				
5								
6	Reserved							ENABLE
7	Reserved							

The LOGICAL UNIT INDEX field contains a value assigned by the DT device at power on that uniquely identifies the ADC logical unit from all other logical units on the DT device, independent of device server. This field shall not be changeable. The ADC device server shall terminate a MODE SELECT command that attempts to change the value in the LOGICAL UNIT INDEX field with CHECK CONDITION status with the sense key to ILLEGAL REQUEST and the additional sense code set to INVALID FIELD IN PARAMETER LIST.

The DEVICE TYPE field shall contain the value shown in table 58 (i.e., 12h, an Automation/Drive Interface device (see SPC-3)).

The ADDITIONAL DESCRIPTOR LENGTH field contains the number of descriptor bytes that follow and shall be set to the value shown in table 58.

The LOGICAL UNIT NUMBER field specifies, for the ADC logical unit when accessed through the DT device primary port(s):

a) the LUN if access controls are not in effect; or
b) the default LUN if access controls are in effect (see SPC-3).

The LOGICAL UNIT NUMBER field contains the first two bytes (i.e., bytes 0 and 1) of a single level logical unit structure or the contents of a two byte extended logical unit address (see SAM-3). The LOGICAL UNIT NUMBER field shall be ignored if the ENABLE bit is set to zero. The ADC device server shall return a CHECK CONDITION status with the sense key set to ILLEGAL REQUEST and the additional sense code set to INVALID FIELD IN PARAMETER LIST to a MODE SELECT command (see SPC-3) when multiple descriptors with the ENABLE bit set to one have the same value in the LOGICAL UNIT NUMBER field.

An ENABLE bit set to one specifies that the DT device primary port(s) associated with the ADC logical unit shall be responsive to commands and task management requests received on the DT device primary port(s). An ENABLE bit set to zero specifies that the DT device primary port(s) associated with the ADC logical unit shall not respond to commands and task management requests received on that DT device primary port(s) and the associated ADC logical unit number shall not be included in the logical unit inventory (see SPC-3) for all I_T nexuses associated with a DT device primary port. The ENABLE bit has no effect on the access to the ADC device server through the ADI port.

If the ENABLE bit is changed from one to zero, then the ADC device server shall implicitly abort all commands in its task set received on a DT device primary port and report CHECK CONDITION status with the sense key set to ABORTED COMMAND and the additional sense code set to LOGICAL UNIT COMMUNICATION FAILURE for each command. All remaining device servers (e.g., local SMC device server, RMC device server) in the DT device shall report a change in the logical unit inventory (see SPC-3) to any application clients connected through a DT device primary port. The ENABLE bit changing from one to zero shall have no effect on commands and task management requests received on an ADI port.

6.2.2.4 Target Device Serial Number subpage

The Target Device Serial Number subpage is variable-length and contains the product serial number of the RMC device server and the ADC device server that shall be reported via the Unit Serial Number VPD page (see SPC-3). This product serial number shall not affect the product serial number of the local SMC device server. The subpage is defined in table 59.

Table 59 — Target Device Serial Number subpage

Bit / Byte	7	6	5	4	3	2	1	0
0	PS	SPF (1b)	PAGE CODE (0Eh)					
1	SUBPAGE CODE (04h)							
2	Reserved							
3	PAGE LENGTH (n-3)							
4	Reserved							MPSN
5	Reserved							
7								
8	PRODUCT SERIAL NUMBER							
n								

See SPC-3 for a description of the PS bit, SPF bit, PAGE CODE field, SUBPAGE CODE field, and PAGE LENGTH field. The SPF bit, PAGE CODE field, and SUBPAGE CODE field shall be set to the values shown in table 59.

The modify product serial number (MPSN) bit and PRODUCT SERIAL NUMBER field are used to modify and report modifications to the product serial number, as defined in table 60.

Table 60 — MPSN field

Code	MODE SENSE command [a]	MODE SELECT command [a]
00b	The MPSN field shall be set to zero for a MODE SENSE command. The PRODUCT SERIAL NUMBER field shall contain the currently assigned value.	Do not modify the product serial number. The PRODUCT SERIAL NUMBER field shall be ignored.
01b	Invalid	Reserved
10b		Set the product serial number to the manufacturer-assigned value. The PRODUCT SERIAL NUMBER field shall be ignored.
11b		Set the product serial number to the value in the PRODUCT SERIAL NUMBER field.
[a] See SPC-3.		

See SPC-3 for a description of the PRODUCT SERIAL NUMBER field. An application client may change the product serial number as a means to change the RMC logical unit's T10 vendor ID based identification descriptor (see SPC-3).

6.3 Security protocol parameters

6.3.1 Security protocol overview

This sub-clause describes the protocols, pages, and descriptors used by automation/drive interface devices with the SECURITY PROTOCOL IN and SECURITY PROTOCOL OUT commands (see SPC-4).

6.3.2 SECURITY PROTOCOL IN command specifying Tape Data Encryption security protocol

The SECURITY PROTOCOL IN command (see SPC-4) specifying Tape Data Encryption security protocol (i.e., 20h) requests the ADC device server to return information about the data security methods in the DT device and on the medium. The command supports a series of pages that are requested individually. An application client requests a page by using a SECURITY PROTOCOL IN command with the SECURITY PROTOCOCOL field set to Tape Data Encryption security protocol and the SECURITY PROTOCOL SPECIFIC field set to the page code requested.

A device server that supports the Tape Data Encryption protocol in the SECURITY PROTOCOL OUT command shall also support a SECURITY PROTOCOL IN command specifying the Tape Data Encryption protocol.

The SECURITY PROTOCOL SPECIFIC field (see table 61) specifies the page that the application client is requesting.

Table 61 — SECURITY PROTOCOL SPECIFIC **field values**

Code	Description	Support		Reference
		ADC Device Server	RMC Device Server	
0000h	Tape Data Encryption In Support page	M	M	SSC-3
0001h	Tape Data Encryption Out Support page	M	M	SSC-3
0002 - 000Fh	Reserved			
0010h	Data Encryption Capabilities page	M	M	SSC-3
0011h	Supported Key Formats page	O	O	SSC-3
0012h	Data Encryption Management Capabilities page	O	O	SSC-3
0013h - 001Fh	Reserved			
0020h	Data Encryption Status page	M	M	SSC-3
0021h	Next Block Encryption Status page	M	M	SSC-3
0022h - 002Fh	Reserved			
30h	Random Number page	O	O	SSC-3
31h	Device Server Key Wrapping Public Key page	O	O	SSC-3
0032h - FEFFh	Reserved			
FF00h - FFFFh	Vendor specific			

Support key:
M - mandatory for device servers that support the Tape Data Encryption security protocol
O - optional for device servers that support the Tape Data Encryption security protocol

If the SECURITY PROTOCOL SPECIFIC field is set to a reserved or unsupported value, then the ADC device server shall terminate the command with CHECK CONDITION status, with the sense key set to ILLEGAL REQUEST, and the additional sense code set to INVALID FIELD IN CDB.

6.3.3 SECURITY PROTOCOL IN command specifying Data Encryption Configuration security protocol

6.3.3.1 SECURITY PROTOCOL IN command specifying Data Encryption Configuration security protocol overview

The SECURITY PROTOCOL IN command (see SPC-4) specifying the Data Encryption Configuration security protocol (i.e., 21h) requests the ADC device server to return information about the data encryption configuration in the device server. The command supports a series of pages that are requested individually. An application client requests a page by using a SECURITY PROTOCOL IN command with the SECURITY PROTOCOCOL field set to Data Encryption Configuration security protocol and the SECURITY PROTOCOL SPECIFIC field set to the page code requested.

A device server that supports the Data Encryption Configuration security protocol in the SECURITY PROTOCOL OUT command shall also support a SECURITY PROTOCOL IN command specifying the Data Encryption Configuration security protocol.

The SECURITY PROTOCOL SPECIFIC field (see table 62) specifies the type of report that the application client is requesting.

Table 62 — SECURITY PROTOCOL SPECIFIC **field values**

Code	Description	Support	Reference
0000h	Data Encryption Configuration In Support page	M	6.3.3.2
0001h	Data Encryption Configuration Out Support page	M	6.3.3.3
0002h - 000Fh	Reserved		
0010h	Report Data Encryption Policy page	O	6.3.3.4
0011h - FEFFh	Reserved		
FF00h - FFFFh	Vendor specific		

Support key:
M - mandatory for device servers that support the Data Encryption Configuration security protocol
O - optional for device servers that support the Data Encryption Configuration security protocol

If the SECURITY PROTOCOL SPECIFIC field is set to a reserved or unsupported value, then the ADC device server shall terminate the command with CHECK CONDITION status, with the sense key set to ILLEGAL REQUEST, and the additional sense code set to INVALID FIELD IN CDB.

6.3.3.2 Data Encryption Configuration In Support page

Table 63 specifies the format of the Data Encryption Configuration In Support page.

Table 63 — Data Encryption Configuration In Support page (part 1 of 2)

Bit / Byte	7	6	5	4	3	2	1	0
0	(MSB)							
1				PAGE CODE (0000h)				(LSB)
2	(MSB)							
3				PAGE LENGTH(n-3)				(LSB)
Data Encryption Configuration In Support page code list								

Table 63 — Data Encryption Configuration In Support page (part 2 of 2)

Bit / Byte	7	6	5	4	3	2	1	0
4	(MSB)	Data Encryption Configuration In Support page code (first)						
5								(LSB)
	. . .							
n-1	(MSB)	Data Encryption Configuration In Support page code (last)						
n								(LSB)

The PAGE CODE field shall be set to 0000h to indicate the Data Encryption Configuration In support page.

See SPC-3 for a description of the PAGE LENGTH field.

The Data Encryption Configuration In Support page code list shall contain a list of pages in ascending order beginning with page code 0000h (see table 61) of all of the pages that the ADC device server supports for the SECURITY PROTOCOL IN command specifying the Data Encryption Configuration security protocol.

6.3.3.3 Data Encryption Configuration Out Support page

Table 64 specifies the format of the Data Encryption Configuration Out Support page.

Table 64 — Data Encryption Configuration Out Support page

Bit / Byte	7	6	5	4	3	2	1	0
0	(MSB)	PAGE CODE (0000h)						
1								(LSB)
2	(MSB)	PAGE LENGTH(n-3)						
3								(LSB)
Data Encryption Configuration Out Support page code list								
4	(MSB)	Data Encryption Configuration Out Support page code (first)						
5								(LSB)
	. . .							
n-1	(MSB)	Data Encryption Configuration Out Support page code (last)						
n								(LSB)

The PAGE CODE field shall be set to 0001h to indicate the data encryption configuration out support page.

See SPC-3 for a description of the PAGE LENGTH field.

The Data Encryption Configuration Out Support page code list shall contain a list of pages in ascending order (see table 69) of all of the pages that the ADC device server supports for the SECURITY PROTOCOL OUT command specifying the Data Encryption Configuration security protocol.

6.3.3.4 Report Data Encryption Policy page

The Report Data Encryption Policy page indicates the current encryption policy configuration for the DT device. Table 65 specifies the format of the Report Data Encryption Policy page.

Table 65 — Report Data Encryption Policy page

Bit / Byte	7	6	5	4	3	2	1	0
0	(MSB)							
1	PAGE CODE (0010h)							(LSB)
2	(MSB)							
3	PAGE LENGTH (8)							(LSB)
4	Reserved				CONTROL POLICY CODE			
5								
6	Reserved							
7	Reserved		DECRYPTION PARAMETERS REQUEST POLICY			ENCRYPTION PARAMETERS REQUEST POLICY		
8	(MSB)							
9	ENCRYPTION PARAMETERS REQUEST PERIOD							(LSB)
10								
11	Reserved							

The PAGE CODE field shall be set to 0010h to indicate the Report Data Encryption policy page.

See SPC-3 for a description of the PAGE LENGTH field.

The CONTROL POLICY CODE field (see table 6) contains information on the data encryption parameters control policy (see table 4.10.1). See 6.3.5.3. for the definitions of the DECRYPTION PARAMETERS REQUEST POLICY, ENCRYPTION PARAMETERS REQUEST POLICY field and the ENCRYPTION PARAMETERS REQUEST PERIOD field.

6.3.4 SECURITY PROTOCOL OUT command specifying Tape Data Encryption security protocol

6.3.4.1 SECURITY PROTOCOL OUT command specifying Tape Data Encryption security protocol overview

The SECURITY PROTOCOL OUT command specifying the Tape Data Encryption security protocol (i.e., 20h) is used to configure the data security methods in the device server and on the medium. The command supports a series of pages that are sent individually. An application client requests to send a page by using a SECURITY

PROTOCOL OUT command with the SECURITY PROTOCOCOL field set to Tape Data Encryption security protocol and the SECURITY PROTOCOL SPECIFIC field set to the page code requested.

The SECURITY PROTOCOL SPECIFIC field (see table 66) specifies the page that the application client is sending.

Table 66 — SECURITY PROTOCOL SPECIFIC **field values**

Code	Description	Support	Reference
0000h - 000Fh	Reserved		
0010h	Set Data Encryption page	O	SSC-3
0011h	SA Encapsulation page	O	SSC-3
0012h - 002Fh	Reserved		
0030h	Data Encryption Parameters Complete	M	6.3.4.2
0031h - FEFFh	Reserved		
FF00h - FFFFh	Vendor specific		

Support key:
M - mandatory for device servers that support the Data Encryption Configuration security protocol
O - optional for device servers that support the Data Encryption Configuration security protocol

If the SECURITY PROTOCOL SPECIFIC field is set to a reserved or unsupported value, then the ADC device server shall terminate the command with CHECK CONDITION status, with the sense key set to ILLEGAL REQUEST, and the additional sense code set to INVALID FIELD IN CDB.

6.3.4.2 Data Encryption Parameters Complete page

Table 67 specifies the format of the Data Encryption Parameters Complete page.

Table 67 — Data Encryption Parameters Complete page (part 1 of 2)

Bit / Byte	7	6	5	4	3	2	1	0
0	(MSB)			PAGE CODE (0030h)				
1								(LSB)
2	(MSB)			PAGE LENGTH(0Ch)				
3								(LSB)
4	AUTOMATION COMPLETE RESULTS							
5	Reserved							
6	Reserved				CABT	CKME	CEPR	CDPR
7	Reserved							

Table 67 — Data Encryption Parameters Complete page (part 2 of 2)

Bit / Byte	7	6	5	4	3	2	1	0
8	(MSB)							
11	PARAMETERS REQUEST SEQUENCE IDENTIFIER							(LSB)
12	Reserved							
15								

The PAGE CODE field shall be set to 0030h to indicate the Data Encryption Parameters complete page.

See SPC-3 for a description of the PAGE LENGTH field.

The AUTOMATION COMPLETE RESULTS field indicates the results of the data encryption parameters request with the request identifier matching the value in the PARAMETERS REQUEST SEQUENCE IDENTIFIER field. The AUTOMATION COMPLETE RESULTS field shall be set to a value specified in table 68.

Table 68 — Automation complete results codes

Code	Description	Additional sense code
00h	No results (e.g., the automation application client has set the CABT bit to one).	n/a
01h	The automation application client has successfully completed servicing the request.	n/a
02h	The automation application client has experienced an unknown error servicing the request.	EXTERNAL DATA ENCRYPTION CONTROL ERROR
03h	The automation application client experienced an unrecoverable error in attempting to access the key manager.	EXTERNAL DATA ENCRYPTION KEY MANAGER ACCESS ERROR
04h	The key manager returned an error status when access to the key was attempted.	EXTERNAL DATA ENCRYPTION KEY MANAGER ERROR
05h	The requested key was not found.	EXTERNAL DATA ENCRYPTION KEY NOT FOUND
06h	A set of data encryption parameters was provided but the DT device was not able to process any logical blocks using the set of data encryption parameters (see 4.10.4.5).	INCORRECT DATA ENCRYPTION KEY
07h	Request not authorized (e.g., the automation application client received an encryption parameters for encryption request and the volume mounted in the DT device does not support encryption but the policy is set to encrypt all data).	EXTERNAL DATA ENCRYPTION REQUEST NOT AUTHORIZED
08 - EFh	Reserved	Reserved
F0h - FFh	Vendor specific	Vendor specific

If the AUTOMATION COMPLETE RESULTS field is set to 00h, then:

a) the clear abort (CABT) bit shall be set to one;
b) the clear key management error (CKME) bit shall be set to one;
c) the clear encryption parameters request (CEPR) bit shall be set to one; or
d) the clear decryption parameters request (CDPR) bit shall be set to one.

The ADC device server shall terminate the command with CHECK CONDITION status, with the sense key set to ILLEGAL REQUEST, and the additional sense code set to INVALID FIELD IN PARAMETERS LIST if the AUTOMATION COMPLETE RESULTS field is set to 00h, and:

a) the CABT bit is set to zero;
b) the CKME bit is set to zero;
c) the CEPR bit is set to zero; and
d) the CDPR bit is set to zero.

The ADC device server shall:

a) set the external data encryption control additional sense code (e.g., see SSC-3) in the DT device to a value specified in table 68; or
b) set the external data encryption control additional sense code in the DT device to EXTERNAL DATA ENCRYPTION CONTROL ERROR.

A clear abort (CABT) bit set to one indicates that the ABT bit in the DT device ADC data encryption control status log parameter shall be set to zero. A CABT bit set to zero does not indicate that the ABT bit in the DT device ADC data encryption control status log parameter shall be set to zero.

A clear key management error (CKME) bit set to one indicates that:

a) the key timeout KTO bit in the key management error data log parameter shall be set to zero;
b) the ERROR TYPE field in the key management error data log parameter shall be set to zero; and
c) the data encryption parameters period expired indicator in the DT device shall be set to FALSE.

A CKME bit set to zero does not indicate that the KME bit in the DT device ADC data encryption control status log parameter shall be set to zero.

If the clear encryption parameters request (CEPR) bit is set to one and the value in the PARAMETERS REQUEST SEQUENCE IDENTIFIER field matches the current data encryption parameters request sequence identifier, then the ADC device server shall set the encryption parameters request (EPR) bit in the DT device ADC data encryption control status log page to zero and shall set the encryption parameters for encryption request indicator in the DT device to FALSE. If the value in the PARAMETERS REQUEST SEQUENCE IDENTIFIER field does not match the current data encryption parameters request sequence identifier, then the ADC device server shall ignore the CEPR bit. If the CEPR bit is set to zero, then the ADC device server is not being requested to clear the encryption parameters for encryption request for the indicated key request sequence.

If the clear decryption parameters request (CDPR) bit is set to one and the value in the PARAMETERS REQUEST SEQUENCE IDENTIFIER field matches the current data encryption parameters request sequence identifier, then the ADC device server shall set the decryption parameters request (DPR) bit in the DT device ADC data encryption control status log page to zero and shall set the encryption parameters for decryption request indicator in the DT device to FALSE. If the value in the PARAMETERS REQUEST SEQUENCE IDENTIFIER field does not match the current data encryption parameters request sequence identifier, then the ADC device server shall ignore the CDPR bit. If the CDPR bit is set to zero, then the ADC device server is not being requested to clear the encryption parameters for decryption key request for the indicated key request sequence.

The PARAMETERS REQUEST SEQUENCE IDENTIFIER field shall contain the data encryption parameters request sequence identifier for the data encryption parameters request that corresponds to these results.

6.3.5 SECURITY PROTOCOL OUT command specifying Data Encryption Configuration security protocol

6.3.5.1 SECURITY PROTOCOL OUT command specifying Data Encryption Configuration security protocol overview

The SECURITY PROTOCOL OUT command (see SPC-4) specifying a value of 21h (i.e., the Data Encryption Configuration security protocol) is used to configure the data security methods in the DT device. The command supports a series of pages that are sent individually. An application client requests to send a page by using a SECURITY PROTOCOL OUT command with the SECURITY PROTOCOCOL field set to Data Encryption Configuration security protocol and the SECURITY PROTOCOL SPECIFIC field set to the page code requested.

The SECURITY PROTOCOL SPECIFIC field (see table 69) specifies the page that the application client is sending.

Table 69 — SECURITY PROTOCOL SPECIFIC **field values**

Code	Description	Support	Reference
0000h - 000Fh	Reserved		
0010h	Configure Data Encryption Algorithm Support page	O	6.3.5.2
0011h	Configure Encryption Policy page	M	6.3.5.3
0011 - FEFFh	Reserved		
FF00h - FFFFh	Vendor specific		

Support key:
M - mandatory for device servers that support the Data Encryption Configuration security protocol
O - optional for device servers that support the Data Encryption Configuration security protocol

If the SECURITY PROTOCOL SPECIFIC field is set to a reserved or an unsupported value, then the ADC device server shall terminate the command with CHECK CONDITION status, with the sense key set to ILLEGAL REQUEST, and the additional sense code set to INVALID FIELD IN CDB.

6.3.5.2 Configure Data Encryption Algorithm Support page

Table 70 specifies the format of the Configure Data Encryption Algorithm Support page. If the DT device has a saved set of data encryption parameters associated with any I_T nexus or a DT device management interface, or has a volume mounted, then the ADC device server shall terminate a SECURITY PROTOCOL OUT command specifying the Configure Data Encryption Algorithm Support page with CHECK CONDITION status and set the sense key to ILLEGAL REQUEST, the additional sense code to INVALID FIELD IN PARAMETER LIST, and the sense key specific FIELD POINTER field set to the PAGE CODE field.

Table 70 — Configure Data Encryption Algorithm Support page (part 1 of 2)

Bit / Byte	7	6	5	4	3	2	1	0
0	(MSB)							
1				PAGE CODE (0010h)				(LSB)
2	(MSB)							
3				PAGE LENGTH(n-3)				(LSB)
4								
19				Reserved				
Encryption Algorithm Support descriptor (first)								

Table 70 — Configure Data Encryption Algorithm Support page (part 2 of 2)

Bit / Byte	7	6	5	4	3	2	1	0
20	Encryption Algorithm Support descriptor (first)							
	. . .							
	Encryption Algorithm Support descriptor (last)							
n								

The PAGE CODE field shall be set to 0010h to indicate the Configure Data Encryption Algorithm Support page.

See SPC-3 for a description of the PAGE LENGTH field.

Each Encryption Algorithm Support descriptor (Table 71) shall contain configuration settings for a data encryption algorithm supported by the DT device. If more than one descriptor is included, then they shall be in ascending order of the value in the ALGORITHM INDEX field. It shall not be considered an error if Encryption Algorithm Support descriptors are not included for all algorithms supported by the DT device.

Table 71 — Encryption Algorithm Support descriptor

Bit / Byte	7	6	5	4	3	2	1	0
0	ALGORITHM INDEX							
1	Reserved							
2	(MSB)	DESCRIPTOR LENGTH (004h)						
3								(LSB)
4	DISABLE	Reserved						
5	Reserved							
7								

The ALGORITHM INDEX field specifies which of the data encryption algorithms reported by the SECURITY PROTOCOL IN command specifying the Tape Data Encryption protocol and the Data Encryption Capabilities pages shall be configured. If the value specified in the ALGORITHM INDEX field is not an algorithm index for a supported data encryption algorithm, then the ADC device server shall terminate the command with CHECK CONDITION STATUS with the sense key set to ILLEGAL COMMAND and the additional sense code set to INVALID FIELD IN PARAMETER LIST.

The DESCRIPTORS LENGTH field indicates the length of the data to follow.

A DISABLE set to one specifies that the DT device shall disable the data encryption algorithm for the algorithm index in the ALGORITHM INDEX field (e.g., return an Encryption Algorithm descriptor for the specified algorithm in response to a SECURITY PROTOCOL IN command specifying the Tape Data Encryption security protocol and the Data

Encryption Capabilities page with the DECRYPT_C field set to no capability and the ENCRYPT_C set to no capability, see SSC-3). A DISABLE bit set to zero specifies that the DT device shall not disable the specified encryption algorithm. If the DISABLE is set to zero, then the DT device shall enable the specified data encryption algorithm.

6.3.5.3 Configure Encryption Policy page

Table 72 specifies the format of the Configure Encryption Policy page.

Table 72 — Configure Encryption Policy page

Bit / Byte	7	6	5	4	3	2	1	0
0	(MSB)							
1	PAGE CODE (0011h)							(LSB)
2	(MSB)							
3	PAGE LENGTH(8)							(LSB)
4	Reserved				CONTROL POLICY CODE			
5	Reserved							
6								
7	Reserved		DECRYPTION PARAMETERS REQUEST POLICY			ENCRYPTION PARAMETERS REQUEST POLICY		
8	(MSB)							
9	ENCRYPTION PARAMETERS REQUEST PERIOD							(LSB)
10	Reserved							
11								

The PAGE CODE field shall be set to 0011h to indicate the configure encryption policy page.

See SPC-3 for a description of the PAGE LENGTH field.

The CONTROL POLICY CODE field specifies the data encryption parameters control policy for the DT device (see 4.10.1). If the DT device has a saved set of data encryption parameters or has a volume mounted the ADC device server shall terminate the command with CHECK CONDITION status, with the sense key set to ILLEGAL REQUEST, and the additional sense code set to INVALID FIELD IN PARAMETER LIST, and the sense key specific FIELD POINTER field set to the CONTROL POLICY CODE field.

Upon successful processing of a Configure Encryption Policy page with the CONTROL POLICY CODE field set to a policy code for the Open policy type or a policy code for the RMC exclusive policy type, then the ADC device server shall:

a) set the encryption parameters request indicator in the DT device to zero;
b) set the decryption parameters request indicator in the DT device to zero;
c) set the encryption parameters request (EPR) bit, decryption parameters request bit (DPR) bit, key management error bit (KME), and the abort (ABT) bit in the DT device ADC data encryption control status log parameter to zero; and

d) set the key timeout (KTO) bit to zero and the ERROR TYPE field to 00b in the key management error data log parameter.

The DECRYPTION PARAMETERS REQUEST POLICY field specifies the policy that the DT device shall use for requesting a set of data encryption parameters for decryption from the automation application client (see SSC-3). The decryption parameters request policy values are defined in Table 73.

Table 73 — DECRYPTION PARAMETERS REQUEST POLICY field values

Value	Policy Name (see SSC-3)	Reference
000b	No data decryption parameters request	SSC-3
001b	Request data decryption parameters as needed	SSC-3
010b - 111b	Reserved	

The ENCRYPTION PARAMETERS REQUEST POLICY field specifies the policy that the DT device shall use for requesting a set of data encryption parameters for encryption from the automation application client (see SSC-3). The encryption parameters request policy values are defined in table 74.

Table 74 — DECRYPTION PARAMETERS REQUEST POLICY field values

Value	Policy Name (see SSC-3)	Reference
000b	No data encryption parameters request	SSC-3
001b	Request data encryption parameters every reposition	SSC-3
010b	Request data encryption parameters when not set	SSC-3
011b - 111b	Reserved	

The ENCRYPTION PARAMETERS REQUEST PERIOD field indicates the maximum time, in 100 millisecond increments, the DT device shall wait after requesting a set of data encryption parameters for encryption (see 6.1.2.4) or requesting a set of data encryption parameters for decryption from the automation application client (e.g., the data encryption parameters period time if the DT device includes an SSC-3 compliant device server, see SSC-3). An ENCRYPTION PARAMETERS REQUEST PERIOD field value of 0000h indicates the data encryption parameters request period shall be infinite.

If the CONTROL POLICY CODE field is set to a policy code for the Open policy type or is set to a policy code for the RMC exclusive policy type, then the DECRYPTION PARAMETERS REQUEST POLICY, ENCRYPTION PARAMETERS REQUEST POLICY, and ENCRYPTION PARAMETERS REQUEST PERIOD fields shall be ignored.

6.4 Vital product data parameters

6.4.1 Vital product data parameters overview and page codes

This subclause defines the vital product data parameters (VPD) pages used with ADC device types. See SPC-3 for VPD pages used with all device types. The VPD page codes specific to ADC devices are specified in table 75.

Table 75 — ADC device VPD page codes

Page Code	Description	Support requirement	Reference
00h	Supported VPD Pages	Mandatory	SPC-3
01h - 7Fh	Reserved		
80h	Unit Serial Number	Mandatory	SPC-3
81h - 82h	Obsolete		
83h	Device Identification	Mandatory	SPC-3 [a]
84h	Software Interface Identification	Optional	SPC-3
85h	Management Network Addresses	Optional	SPC-3
86h	Extended INQUIRY Data	Optional	SPC-3
87h	Mode Page Policy	Optional	SPC-3
88h	SCSI Ports	Optional	SPC-3
89h - B0h	Reserved		
B1h	Manufacturer-assigned Serial Number VPD page	Optional	6.4.3
B2h - BFh	Reserved		
C0h - FFh	Vendor specific		

[a] See 6.4.2.

6.4.2 Device Identification VPD page

The ADC device server shall either:

a) not return the T10 vendor ID descriptor (see SPC-3) with an ASSOCIATION field set to 00b (i.e., logical unit); or
b) ensure that the T10 vendor ID descriptor with an ASSOCIATION field set to 00b (i.e., logical unit) be unique (e.g., by including “ADC” within the VENDOR SPECIFIC IDENTIFIER field).

6.4.3 Manufacturer-assigned Serial Number VPD page

Table 76 defines the Manufacturer-assigned Serial Number VPD page.

Table 76 — Manufacturer-assigned Serial Number VPD page

Bit / Byte	7	6	5	4	3	2	1	0
0	PERIPHERAL QUALIFIER			PERIPHERAL DEVICE TYPE				
1	PAGE CODE (B1h)							
2	Reserved							
3	PAGE LENGTH (n-3)							
4	MANUFACTURER SERIAL NUMBER							
n								

See SPC-3 for a description of the PERIPHERAL QUALIFIER field, PERIPHERAL DEVICE TYPE field, PAGE CODE field, and PAGE LENGTH field. The PAGE CODE field shall be set to the value shown in table 76.

The MANUFACTURER-ASSIGNED SERIAL NUMBER field contains right-aligned ASCII data (see SPC-3) that is the manufacturer-assigned serial number. If the manufacturer-assigned serial number is not available, then the ADC device server shall return ASCII spaces (20h) in this field. If the manufacturer-assigned serial number differs from the value in the PRODUCT SERIAL NUMBER field (see SPC-3), then the manufacturer-assigned serial number shall not be used in building the T10 vendor ID descriptor (see SPC-3).